Designing an Application Centric Network for the $1.9 Trillion Internet of Things Economy

From healthcare to automotive and manufacturing to consumer electronics, the Internet of Things is a quantum revolution in how we think about application data connectivity. Make sure your network is ready for the application onslaught of the $1.9 trillion* Internet of Things economy.

GET READY FOR THE INTERNET OF THINGS

The Internet of Things (IoT) is all the rage. It's the buzzword de jour. Whether its lauded in the popular press, technology journals or industry conference keynotes, it's hard to escape the moniker and very easy to dismiss IoT as hype about smart refrigerators that remind you to buy more milk. It's more than that, way more. Gartner projects that the Internet of Things will bring a total economic value-add of $1.9 trillion by 2020, and the number of connected devices will reach 26 billion, while information managed by enterprises will grow by 14x.

IoT comprises every end node on the Internet and private network and the servers those central systems connect to in the private or public cloud. In Gartner's definition, that includes things that are not necessarily connected directly to the public Internet, but they must be connectable via a network (which could be a LAN, PAN, body area network, etc.) and individually addressable.

WHAT MAKES IoT DIFFERENT?

IoT extends the end node far beyond the human-centric world to encompass specialized devices with human-accessible interfaces, such as smart home thermostats and blood pressure monitors, and even those which lack human interfaces altogether, including industrial sensors, network-connected cameras and traditional embedded systems.

As IoT grows, the need for real-time scalability to handle dynamic traffic bursts also increases. There may be the need to handle very low bandwidth small data streams, such as a sensor identifier and a status bit on a door sensor or large high-bandwidth streams, like high-def video from a security camera. There is almost always the need for encryption as well.

The scope of IoT is huge. In some cases, the end node may be a low-powered embedded microcontroller with sensors, hard wired to an industrial network and running 24/7.

*Gartner Forecast: The Internet of Things Worldwide, 2013

Network-connected devices are exploding in number, locations, functionality, and expectations. Consider the following examples and their applicability to IoT:

HOSPITALS

Hospitals utilize several smart devices, both standalone and those wired to nurses' station monitors. Soon these will be interconnected through a highly available and secure network with server-based applications that can track patient conditions by correlating all data - not just nurses' readings - allowing better monitoring, data logging and Big Data analytics. Staff will be able to focus on delivering the best care based on deterministic information. An IoT-connected network helped St. Luke's Medical Center reduce patient-bed turnaround time by 51 minutes.

FACTORIES & WAREHOUSES

The flow of materials must be monitored and optimized for efficiency. Location sensors are embedded in components moving through assembly lines and inventory systems. The location of forklifts, pallets and workers are tracked as well, while centralized software directs and redirects the activity in real time to effectively respond to customer requests. By implementing predictive maintenance along with quality control IoT, BMW reduced auto-warranty costs by 5% and reduced the scrap rate of defective vehicles by 80%.

HOMES & OFFICES

Utility meters send complex data packets to service providers where centralized systems provide real-time monitoring to proactively detect & remediate problems such as blackouts, water leaks and circuit overloads. Data is analyzed to improve efficiency by determining needs, spotting trends, and predicting demand. By virtue of its smart IoT fixtures, the city of Oslo reduced energy costs by 62%.

WEARABLES

From heartbeat-sensing fitness bands to step-counting smartphone apps, wearables are the public face of IoT. A portable device is connected to a service that aggregates data and, increasingly, shares it across social media, with a doctor or even a gym. The cloud-based services also push back analytics, motivational graphics and music, and location-based maps.

A Key Ingredient: Dynamic Application Delivery

Dynamic application delivery is an essential component in the design of local-area networks, private clouds and public hosting platforms. Consider a load balancer as a dispatcher, assigning work to thousands of application servers based on the amount of end-node traffic. The server could be software running in a physical data center or a virtual machine in the cloud, dynamically provisioned when additional resources are required and terminated when those needs subside.

Another IoT critical component is how application performance and data movement are handled. When an IoT node performs a service request, such as sending a medical data packet, the ADC (application delivery controller) determines which server, virtual or physical, can handle the request. The packet is then sent to the appropriate server for processing, while measuring the performance of the application and other important data points that determine high availability. But that's not all application delivery technology does. It can also remember which application server is handling a specific IoT node's service requests. When subsequent packets arrive from the same IoT node as part of the same request, the session will continue with the same server, ensuring continuity of the traffic stream and reducing the need for renegotiation.

A core part of an application delivery controller's responsibility is to monitor the health of application servers. Common statistics are processor and memory utilization, server response time, and how different protocols are handled. When the servers slow down or become unresponsive, advanced load balancers dynamically route traffic to other servers. The ADC transfers existing service requests to other servers in order to reduce client interruption. An ADC is a mission-critical tool that enables the full scalability and reliability of the Internet of Things. As the world of IoT evolves and expands, so do the capabilities of application load balancing technologies.

The evolution of the modern load balancer

Modern load balancers focused on application delivery are more sophisticated and operate from Layer 4 to the Application Layer 7, making them more in tune with application server software, how the client responses should be handled, and the specific services being requested by IoT end nodes. ADCs provide packet encryption/decryption, reducing server workload and making it possible to apply advanced policies and processing on secured traffic streams while maintaining end-to-end security. Global Server Load Balancing (GSLB) allows the intelligent distribution of end node traffic across private and public clouds based on proximity, performance or manually defined business rules for optimal data handling and communication. To facilitate the dynamic cloud infrastructure, modern ADCs have also been adapted to integrate into virtual environments.

With simple configuration and portability, virtual ADCs meld seamlessly into private clouds with hypervisor so administrators can launch applications quickly. Since these are application-centric focused, IoT users are assured that instances virtual environments support are functioning as they should, not just in the context of being a VM, but for the application they are serving. NFV (Network Functions Virtualization) de-couples basic network functions, including firewalling, Network Address Translation (NAT), load balancing and security filtering from running in hardware and Application Specific Integrated Circuits (ASICs) to run in software, making it easy to increase scalability and boost performance as administrators or automation software can quickly and easily allocate new resources. Since IoT encompasses devices that could be anywhere, connected via any network, the ability to replace costly hardware in fixed locations with software provides optimum flexibility. NFV services can be configured on the fly, so management software can dynamically improve the user experience and meet QoS requirements.

NFV service chaining refers to all of the virtual and physical devices and software based services required to connect all parts of an application, from the router to load balancer to multiple application servers, database servers, Web servers and other NFV services like WAF (web application firewall). There may be many IoT devices scattered across data centers and cloud providers. Provisioning and monitoring the service chain is costly and time-consuming, especially with proprietary networking hardware, a variety of operating systems, and a mix of vendor-specific management tools. Service chaining is more easily enabled with NFV because virtualized network functions can be provisioned and re-provisioned entirely through software to support the workload or customer requirements. These technologies – advanced load balancers or ADCs, NFV and service chaining – are well-suited for the ever-growing Internet of Things economy.

The Internet of Things is Now!

The Internet of Things is not just the connected refrigerator. It's thousands of medical devices in hospitals; smart utility meters; GPS-based location systems; fitness trackers; toll readers; motion detector security cameras; smoke detectors; and last, but not least, embedded systems.

Each of those IoT end nodes requires connectivity, processing and storage, some local, some in the cloud. This means scalability, reliability, security, compliance and application elasticity to adapt to dynamic requirements and ever-changing workloads.

Now is the time for network administrators to fully scope out all of their 'Internets' and how everything interconnects, from how ERP software systems maintain monitoring rules and governance to how APIs talk to M2M application platforms, as well as how asset and device management mechanisms orchestrate version control and location metrics.

CHALLENGES TO ENABLING IoT

An IoT application may have hundreds, thousands, or even millions of participating devices. Sometimes the number of connections & the amount of data will be consistent and predictable, but not always. Here are a few of the more pressing challenges to providing the back end connectivity & customer satisfaction in IoT applications:

HANDLING HUGE AMOUNTS OF TRAFFIC INCLUDING BURSTS

A motion detector video camera maintains a minimal connection to a cloud-based application server, perhaps a periodic "heartbeat" packet that provides operational status. When the motion detector is tripped, the camera suddenly kicks into gear and transmits streams of high definition video to be stored and analyzed. Imagine the burst of data coming from, say, runners wearing fitness bands at a sporting event like the New York City Marathon. IoT systems designers should plan to manage any quantity of data in unpredictable bursts without dropping packets, overloading the network or overwhelming servers – all while accommodating the BI analytics software required to make sense of the data, often in real time.

MAINTAINING FAST RESPONSE TIME & QUALITY OF SERVICE

Consumers and employees expect fast response time to their mobile apps. So do embedded industrial applications. A warehouse application that directs workers to pick up and deliver materials is a failure if it freezes or if is slow to process location-awareness packets. The server infrastructure and network design of an IoT application needs to be focused on both maintaining fast response time and ensuring robust Quality of Service (QoS), especially in real time location-aware applications.

SECURITY, PRIVACY AND REGULATORY COMPLIANCE

Whether an IoT application is industrial or consumer, enterprise or personal, data must be protected in transit and at rest. Applications store current and historical data about an individual's health, location and finances as well as trade secrets, such as the location and quantity of inventory, business orders and more. This includes ankle sensors on criminals and heart monitors for patients. Data must be secured against theft and tampering. This can be challenging when data is transmitted across the Intenet or even secured private networks and VPN tunnels. Government regulations such as HIPAA or restrictions on transporting data across international borders may also apply. Key IoT security tasks will be to ensure that proper application-level protections, such as DDoS attack mitigation, reach out to end-points and incorporate measures confirming the identity of entities requesting access to data, including multi-factor authentication.