Development Considerations for Smart Cells

Larry Donahue
Technical Specialist,
Intel Corporation

The wireless industry has embraced small cell base stations as a cost-effective way to deploy additional network capacity in saturated locales and increase coverage in other areas. Moving forward, small cells will become more intelligent, making them "smart cells." Smart cells will help lower operational expenses through advanced services, such as data caching, and through offloading backhaul traffic from the wireless carrier's access network to a customer premises, broadband connection. Other advanced services like local ad insertion will provide new revenue opportunities as well. For wireless operators, increasing the intelligence in the radio access network (RAN) lays the groundwork for new revenue-generating services and improved network utilization, and hence, greater profitability.

Smart cells have to be a cut above their predecessors; from the perspective of network operators, this means simplifying new service deployment, adapting better to future requirements and defending against evolving security threats. Smart cell developers have to strike the right balance between these requirements and overall product cost, given the cost-sensitive nature of this equipment segment.

Simplifying the Deployment of New Services

A major challenge for wireless operators in providing a uniform, consistent end user experience is the diverse set of locales with varied geographic and network characteristics. For example, network deployments in dispersed rural areas have different requirements than densely populated, urban areas with respect to the number of subscribers, coverage area for a given base station, radio technologies deployed, number of sectors and the like. Moreover, backhaul capabilities range from regions with high bandwidth fiber deployments to those with more traditional circuit switched networks.

REQUIREMENT: Network operators want to be able to easily reuse the software, delivering new services across different radio access network (RAN) deployments supported by smarts cells, traditional macro cells and eNodeBs. In this way, every subscriber can benefit from the rollout of new capabilities in a timely manner. In addition, effective software reuse can dramatically reduce the non-recurring engineering (NRE) expenses of developing and deploying these services.

DESIGN CONSIDERATIONS: A major impediment to software reuse in the RAN and the network core is the lack of platform consistency, particularly processor architecture and operating systems, across network elements. As a result, the optimized code written for one network element is not likely to port easily to another network element due to platform differences. However, with advances in processor architecture and silicon technologies, it's possible for a given processor architecture to scale across these network elements. Today's smart cell developers should think about prioritizing scalability in order to enable network operators to more easily reuse services across network elements. Still, achieving this objective requires a processor

architecture that can scale from "big iron" core network elements down to cost-sensitive smart cells.

Satisfying such a wide range of traffic throughput and application performance, Intel® architecture scales from multi-core Intel® Xeon® processors for the packet core (for example, serving gateways) to single core Intel® CoreTM processors and Intel® AtomTM processors for fanless smart cell base stations. The architecture also permits scaling across RAN network elements from multi-core Intel Xeon processors in the Cloud RAN to Intel Core processors for eNodeBs and smart cell base stations, and on to Intel Atom processors for very power-efficient smarts cells. This consistency of architecture enables applications written for the mobile core network to be reused, not only across the core network, but also into the RAN, and vice versa. Further facilitating software reuse, Intel architecture processors support virtualized environments, such that an application and its native operation can be moved via a virtual machine with minimal or no software modifications.

VIRTUALIZATION: Virtualization has a long, successful track record of lowering the total cost of ownership in corporate and telecom data centers. IT departments, faced with the challenge of maintaining older, outdated server platforms, can port the associated software to a single physical server that is capable of hosting many applications each running on its own virtual machine, or VM (Figure 1). As a result, there are fewer systems to power and maintain, which reduces data center operating costs. In addition, it's possible to give an application more computing capacity in minutes, whereas before virtualization, it may have taken weeks to acquire a new server. Re-validation efforts are minimal because IT departments can simply migrate a legacy application (along with its operating system and operating environment) to a virtual machine.

Virtualization can bring a variety of benefits to the RAN since it is an enabling technology that helps make platforms more scalable, future-proof and, as discussed later, more secure. Virtualization makes software applications, like data caching and other location based services, more portable, allowing operators to scale services across smart cells, macro cell base stations and cloud-based RANs supporting multiple radio resource modules.

Adapting to Future Requirements

With the industry facing an exponential increase in mobile traffic in the coming years, network operators will be forced to squeeze every last bit of bandwidth from network equipment. The industry is responding to the trends with LTE, which provides almost eight times more uplink bandwidth than its predecessor, High Speed Packet

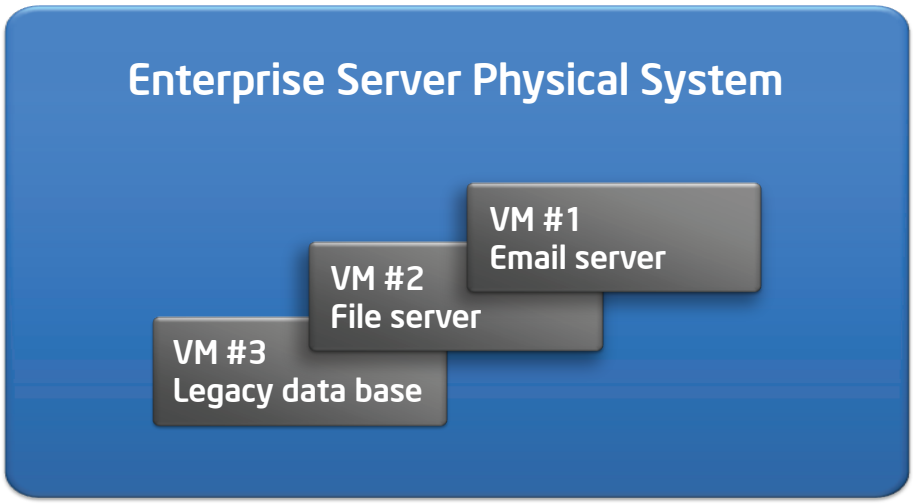

Figure 1. Virtualization Enables Application Software Consolidation

Access (HSPA). Sitting at the network edge, smart cells will be expected to push more and more bits while delivering value-added, revenue-generating services.

REQUIREMENT: As LTE builds out, network elements will be called upon to handle more traffic and support emerging services, which will require higher levels of packet processing and general-purpose computing performance, respectively. Network operators will continue to value equipment with headroom (spare capacity) because it extends a network element's useful lifetime.

DESIGN CONSIDERATIONS: System developers must decide where to process networking workloads (e.g., L3 forwarding), and the principle choices are in purpose-built accelerators or in software. Accelerators generally provide a performance advantage over software-only implementations, but at the expense of higher development cost and lower flexibility. Accelerators are designed and optimized for a particular set of tasks, which limits their ability to accommodate future requirements.

Packet processing, once primarily run on purpose-built hardware, can now be executed on general-purpose Intel architecture processors with impressive results. The Intel® Data Plane Development Kit (Intel® DPDK) contains performance-tuned software libraries developed specifically for packet processing to run on general-purpose CPU cores as well as on accompanying acceleration hardware. A major benefit from this approach is that a smart cell based on an Intel Atom processor can perform packet processing on one processor core and execute application software on another. When a network operator needs to support a new feature, the base platform does not change. Equipment manufacturers using the Intel DPDK can focus their development resources on the higher OSI layers where they can differentiate their products from the competition and provide greater value to their customers.

For higher performance network elements, a dual Intel® Xeon® processor E5-2600 series platform is capable of processing 160 million packets per second (MPPS) of L3 forwarding.[1,2] When the Intel® Communications Chipset 89xx Series is added to the platform, 80 gigabits (Gbps) per second of IPSec acceleration[1,2] has been demonstrated. Developers can assign processor cores to packet and application processing as they see fit, or the platform can be designed to allocate processor cores to different workloads in real time.

Defending Against Evolving Security Threats

Network operators have a great deal of concern and apprehension about what it takes to secure their networked equipment, and rightfully so. In the first quarter of 2012 alone, an astonishing eight million new malware samples were detected.[3] Operators deploying new services, whether home grown or from independent software vendors (ISVs), must be extremely careful about introducing new vulnerabilities to the network. All network elements, including smart cells, must actively protect themselves against known and zero-day threats.

REQUIREMENT: Wireless service providers must keep their networks secure. However, opening up a service provider's network to various applications from an ecosystem of ISVs appears to run counter to the goal of keeping its network secure and represents a nontrivial challenge for the system developer. How can a system be open to an ecosystem of innovative software developers, yet stay safe and secure?

DESIGN CONSIDERATIONS: In addition to facilitating workload consolidation, virtualization technology can be used to enhance the security of a system. Hardware-based virtualization can run different workloads in secure partitions, such that unintended interactions (e.g., unauthorized memory accesses) are prevented by hardware mechanisms that provide enhanced protection over page tables and other low level constructs. For instance, smart cell developers can protect critical control

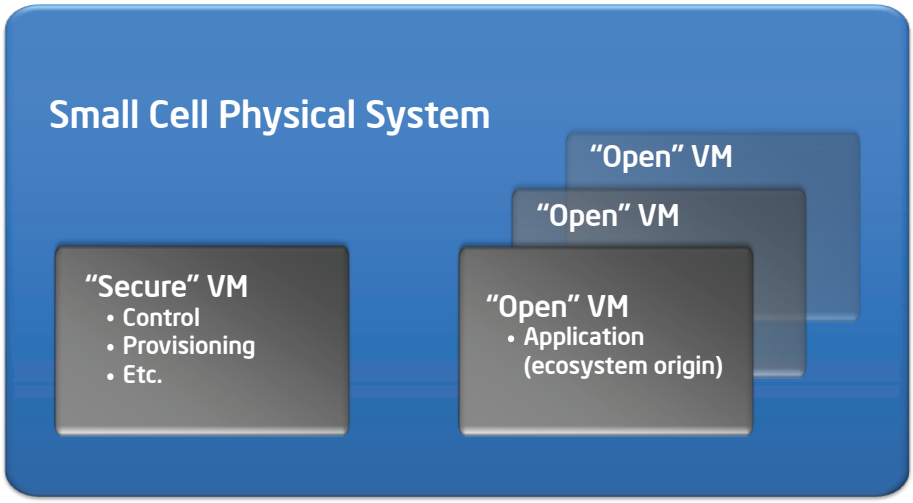

Figure 2. Applications Run in Secured Partitions Called Virtual Machines

functions by running them in their own virtual machines, as shown in Figure 2; this isolates critical functions from other application code (running in other virtual machines) that may be susceptible to malware.

Another layer of protection against malware is called application whitelisting, a lesser known alternative to anti-virus (AV) software. Whitelisting ensures only authorized, trusted software (i.e., whitelist) is permitted to execute; and conversely, unknown and malicious code is blocked without requiring signature files. Once the whitelist is created and enabled, the system is locked down to the known good baseline. Whitelisting, as implemented by McAfee* Embedded Control, is particularly effective and efficient for fixed function devices, such as network elements, which generally run a pre-defined set of applications.

Intel® Trusted Execution Technology (Intel® TXT)[4] offers additional security against software-based attacks in a virtualized deployment. The technology establishes a hardware-based trusted software execution environment that verifies launch-time components and allows only "known good" configurations of critical software to control the platform. Intel TXT integrates security capabilities into the processor, chipset and other platform components. These hardware-based security features, unalterable by rogue software, further protect virtual machines and crucial platform data, and keep malware from launching in the first place.

Intel® Virtualization Technology (Intel® VT)[5] for IA-32 Intel® Architecture (Intel® VT-x) and Intel TXT provide hardware-based mechanisms to virtualize and protect application execution with the aim of delivering the level of security required by network operators. Intel VT is available on various products across the spectrum of Intel's offerings – Intel Atom, Intel Core and Intel Xeon processors – and besides adding another layer of security protection, it helps to increase scalability and code reuse across smart cells, macro cell base stations, cloud-based RAN and beyond.

Summary

The evolving wireless network is driving smart cell developers to consider new ways to simplify new services deployment, adapt to changing requirements and protect against emerging security threats. Addressing these challenges is made easier by the large family of scalable Intel architecture processors with common instruction set, enhanced packet processing capabilities, and virtualization and security technologies.

For more information about Intel solutions for the communications industry, visit www.intel.com/go/commsinfrastructure

[1] Performance estimates are based on internal Intel analysis and are provided for informational purposes only.

[2] Performance tests and ratings are measured using specific computer systems and/or components and reflect the approximate performance of Intel® products as measured by those tests. Any difference in system hardware or software design or configuration may affect actual performance. Buyers should consult other sources of information to evaluate the performance of systems or components they are considering purchasing. For more information on performance tests and on the performance of Intel products, visit http://www.intel.com/performance/resources/limits.htm

[3] http://www.mcafee.com/us/about/news/2012/q2/20120523-01.aspx.

[4] No computer system can provide absolute security under all conditions. Intel® Trusted Execution Technology (Intel® TXT) requires a computer system with Intel® Virtualization Technology (Intel® VT), an Intel TXT-enabled processor, chipset, BIOS, Authenticated Code Modules and an Intel TXT-compatible measured launched environment (MLE). The MLE could consist of a virtual machine monitor, an OS or an application. In addition, Intel TXT requires the system to contain a TPM v1.2, as defined by the Trusted Computing Group and specific software for some uses. For more information, see http://www.intel.com/technology/security.

[5] Intel® Virtualization Technology (Intel® VT) requires a computer system with an enabled Intel® processor, BIOS, virtual machine monitor (VMM), and for some uses, certain platform software enabled for it. Functionality, performance, or other benefits will vary depending on hardware and software configurations and may require a BIOS update. Software applications may not be compatible with all operating systems. Please check with your application vendor.

Printed in USA MS/VC/1112 Order No. 328182-001US