Cisco Cloud Core
Challenges and Benefits of a Cloud Native 4G and 5G Core

Aeneas Dodd-Noble
Principal Engineer
November 2018
Evolution of the Workloads

- **Hardware**
  - **Host OS**
  - **Runtime**
  - **App**

<table>
<thead>
<tr>
<th>Bare Metal / Dedicated</th>
<th>Virtual Machine</th>
<th>Containers in VM</th>
<th>Containers (on BM)</th>
</tr>
</thead>
<tbody>
<tr>
<td>H.OS / Hypervisor</td>
<td>H.OS / Hypervisor</td>
<td>H.OS / Hypervisor</td>
<td>H.OS / Hypervisor</td>
</tr>
<tr>
<td>OS</td>
<td>OS</td>
<td>OS</td>
<td>OS</td>
</tr>
<tr>
<td>VM</td>
<td>VM</td>
<td>VM</td>
<td>VM</td>
</tr>
<tr>
<td>Hardware</td>
<td>Hardware</td>
<td>Hardware</td>
<td>Hardware</td>
</tr>
</tbody>
</table>

**Worldwide Container Instances Installed Base by Virtualized/Non-Virtualized (excluding web/SaaS provider internal infrastructure), 2015–2020**

- Virtualized
- Non-Virtualized

© 2018 Cisco and/or its affiliates. All rights reserved.
- Microservices
  - Modular, loosely coupled software services
  - Individually deployed and lifecycle managed
- Containers
  - Virtualization and management of Microservices
  - Highly portable to different deployment targets
- Continuous Delivery
  - Automated continuous integration, validation and availability of containers
- DevOps
  - Automate and manage rapid deployments
  - Isolate production changes and deploy once validated
Architecture Transition

Appliance
- CMTS
- EPC
- Router

Virtual
- vCCAP
- vEPC
- vRouter

Cloud Native
- Cloud Native Broadband Router
- Cloud Native EPC
- Cloud Native BNG
End Customer Benefits of Virtualization and CN

- Features are provided at web speed
  - 3rd party integration is simplified
- Network resources are efficiently used
- Services can be turned up, tested and made available in 5 minutes
- Integration is driven by shared APIs instead of MIB’s and CLI
- Telemetry provides greater insights on usage, problems and areas of focus
- Subscribers have their can own their highly customized network
- Functions are decentralized, global and local
Cloud Native Benefits

- **Lifecycle Automation**: Automated instantiation and placement, upgrade, scale and recovery.
- **Multi-Cloud Portability**: Mobile core disaggregation to the edge across public, private, and hybrid clouds.
- **Lightweight and Fast**: Extremely fast startup times improves recovery and scaling event handling. Easy to develop at speed.
- **High Performance**: Bypass the hypervisor overhead when deployed on bare metal. VPP based forwarding plane and vswitch.
- **Stateless Application Services**: State services are separated from the application processing to simplify manageability.
Process Separation

Monolithic Software

- S5
- S2a
- S2b
- Sxb
- SGi
- PGW
- Gx
- Gy
- AAA
- OAM
- Gz

State and application are in single process

Microservice Container Software

- N4
- Nsmf
- Front end
- Front end
- Logging
- Tracing
- Common Data Layer
- Data Store
- Stateless Applications
- State Data Store

© 2018 Cisco and/or its affiliates. All rights reserved.
Control Plane 3-tier Architecture State Separation

Service Mesh/Protocol LBs

- Dynamic Discovery of application containers
- Protocol proxy and/or termination, e.g., Diameter, GTP, HTTP2
- Stateless services

Application Services

- Core application/business logic
- Varying degrees of Microservice granularity
- Native scale out and upgrade
- Stateless services

State Management Services

- State separation layer
- Supports different data storage technologies – in memory caches to full fledge DBs
- Scale out technologies
Packing In the Containerized Slices

SMF and PCF VNF VM’s deployed on 50% of the server on multiple servers

Multiple SMF, PCF and other VNFs for a slice deployed on the multiple servers

SMF and PCF VNF VM’s deployed on 50% of the server on multiple servers

Multiple SMF, PCF and other VNFs for a slice deployed on the multiple servers
Containerizing Use Plane
Cloud Native & Vector Packet Processing Plug Ins
Container Service Chaining
5G UPF CN Architecture

- UPF optimized with inline services
- Loosely coupled 3rd party Proxy for specific use-cases
- Common N4+ CP interface
- Managed as a single VNF
- Common Vector Packet Processing Fast Path Arch
- K8/container orchestration and LCM
Operational Challenges
Must View Critical Infrastructure Differently
Pets vs. Livestock

Bill Baker (Microsoft), Randy Bias (CloudScaling), Tim Bell (CERN)
http://cloudscaling.com/blog/cloud-computing/the-history-of-pets-vs-cattle/
SP Stack for Cloud Native Network Functions

Common Functions
- Authorization
- Service Discovery
- Configuration
- Metrics/Monitoring
- Security

Automation
- Automation Services
- Infrastructure Access
- App/Control Plan Services
- User / Data Plane Services

Cloud Native Stack
- App Infr.

Infrastructure
- Cloud Native Orch / Services
- Infr Services

Container Networking
- Container Orchestration / Engine
- Bare Metal aaS
- openstack
Typical Open Source Utilities

- Messaging: Kafka between consumers and producers
- Data store: Redis, Mongo or Cassandra
- Service mesh: Istio
- Logging: Often ELK stack is used with fluentd
- Health and status: Prometheus, Grafana and OpenTrace, Jaeger
- Security: Vault is used for storing certificate and M-TLS for encryption
- Orchestration: Kubernetes and Docker containers.
Dedicated vs Shared Services Within a K8s Cluster

- There are 2 types of services
  - Application Specific
  - Common Services

- If the infrastructure already provides the common set of services then the cloud native application can be installed only with application specific services
Service Mesh – Intelligent Routing & Load Balancing

Changes are controlled and managed by the Service Mesh connecting containers.

The Service Mesh consists of two planes:
- The “data plane” refers to the proxy function in front of each container, accepting traffic.
- The “control plane” refers to a central service (configuration) that manages the rules for the service proxies.

Service Mesh
- Traffic Management
  - Routing rules on labels and L7 AVPs
  - msisdn, imsi, supi, apn
- Metrics – track flow of traffic between services
- Security - Enforces security, access, and isolation.
- Auto-discovery for new Containers and Services
- On-the-fly, surgical control of service routing
- Can apply weighted load balancing rules
- Can retain stickiness for existing sessions

© 2018 Cisco and/or its affiliates. All rights reserved.
3GPP eSBA Service Framework

Extract from TR 23.742

Solution 4: Distributed 3GPP Aware Service Framework

Note: R16 is still in study phase and this architecture is not finalized
Life Cycle Management
Cloud Native DevOps Lifecycle

Build
- Code
  - Automated Test
  - Automated Build
  - Automated Install

Automated Gate

Validate
- Continuous Integration
  - Continuous Delivery
  - Continuous Deployment

Automated Gate

Ship

Run
- Auto Scaling
- Continuous Monitoring
- Continuous Updates

Automated Gate

Cloud Native Needs

- Frequent automated deployments and updates

Bare Metal
Private Cloud
Public Cloud

© 2018 Cisco and/or its affiliates. All rights reserved.
Evolving Automated Upgrades

**Manual Software Upgrades**

**STEP 01**
Manual MOP execution

**STEP 02**
Mass upgrade impacting all sessions

**STEP 03**
Verify to see if everything went ok

**STEP 04**
If it fails, begin rollback of software

**Automated, Incremental Upgrades**

**STEP**

- Instantiate a new VNF instance with the upgraded software
- Direct a small portion of the subscribers/sessions to the upgraded VNF
- Monitor the upgraded VNF & verify key KPIs
- Incrementally add more sub. / sessions to the upgraded VNF
- Canary
- Retire original VNF instance once all sub. have been migrated

**Complex Operation**

**Highly Risky**

**Too Many Admins**

**Step 01**

Manual MOP execution

**Step 02**

Mass upgrade impacting all sessions

**Step 03**

Verify to see if everything went ok

**Step 04**

If it fails, begin rollback of software

**Automated, Incremental Upgrades**

- Instantiate a new VNF instance with the upgraded software
- Direct a small portion of the subscribers/sessions to the upgraded VNF
- Monitor the upgraded VNF & verify key KPIs
- Incrementally add more sub. / sessions to the upgraded VNF
- Canary
- Retire original VNF instance once all sub. have been migrated

**Complex Operation**

**Highly Risky**

**Too Many Admins**
Canary Upgrade – 10% Traffic Diversion to upgraded software
Canary Upgrade – 100% Traffic Diversion to upgraded software
Security in Virtual and Cloud
Trustworthy Systems Architecture

**Foundation of Trust**

- Secure Process
  - Lifecycle / Security Baseline
  - Common Modules & Hardware
    - Trust Anchor
    - Secure Boot
    - Entropy
    - Immutable Identity
    - Image Signing
    - Common Crypto
    - Secure Storage
    - Run Time Integrity

- Trustworthy Systems Technology
  - Common Crypto
  - Secure Storage
  - Run Time Integrity

- Secure Standards
  - Information Assurance (IA)
    - Common Criteria
    - ISO 27034
    - FIPS / USGv6
    - TCG

© 2018 Cisco and/or its affiliates. All rights reserved.
Containers Pose Additional Challenges

- The risk of privilege escalation via containers. If get root inside a containerized app, could gain root access to the host system.

- An attack originating from one container that compromises data or resources used by a different container.

- Simple DoS attacks where one container seizes control of all available system resources in order to stop other containers from operating properly.

- Risk of insecure or unvalidated app images. If access apps from a public repository, there is a risk that you’ll get an image containing malicious code.
Container Security Concerns

**Dev**
- Scan for image vulnerabilities
- User access control

**Test**
- Image change mgmt.
- Harden the host config.
- User access control

**Run**
- Monitor container behavior
- Detect/prevent intrusion
- User access control
It is worth it

Convergence
- Wired and wireline technologies combine
- Same deployment and lifecycle management

Scale
- Auto scale out and in
- Small to enormous
- Deploy at edge and around the world

Portable
- Runs on VM’s, baremetal, public and private cloud
- Same process for all deployment options

Operational and Cultural Shift
- Rapid time from idea to deployment
- Skilled operational team

Innovate at Lower Cost
- Grab new opportunities when they appear
- Personalize experiences and increase value to customers