



OPEN NETWORKING
SUMMIT 2016

MARCH 14-17, 2016 | SANTA CLARA, CA

Challenges and Solutions for Testing NFV/SDN Networks

Trinh Vu, *Amdocs Inc.*

March 16, 2016

Agenda

CSP NW
Environment

NFV/SDN
Advantages

NFV/SDN
Challenges

NFV NW
Design and
Development

NFV NW
Testing

NFV Common
Issues

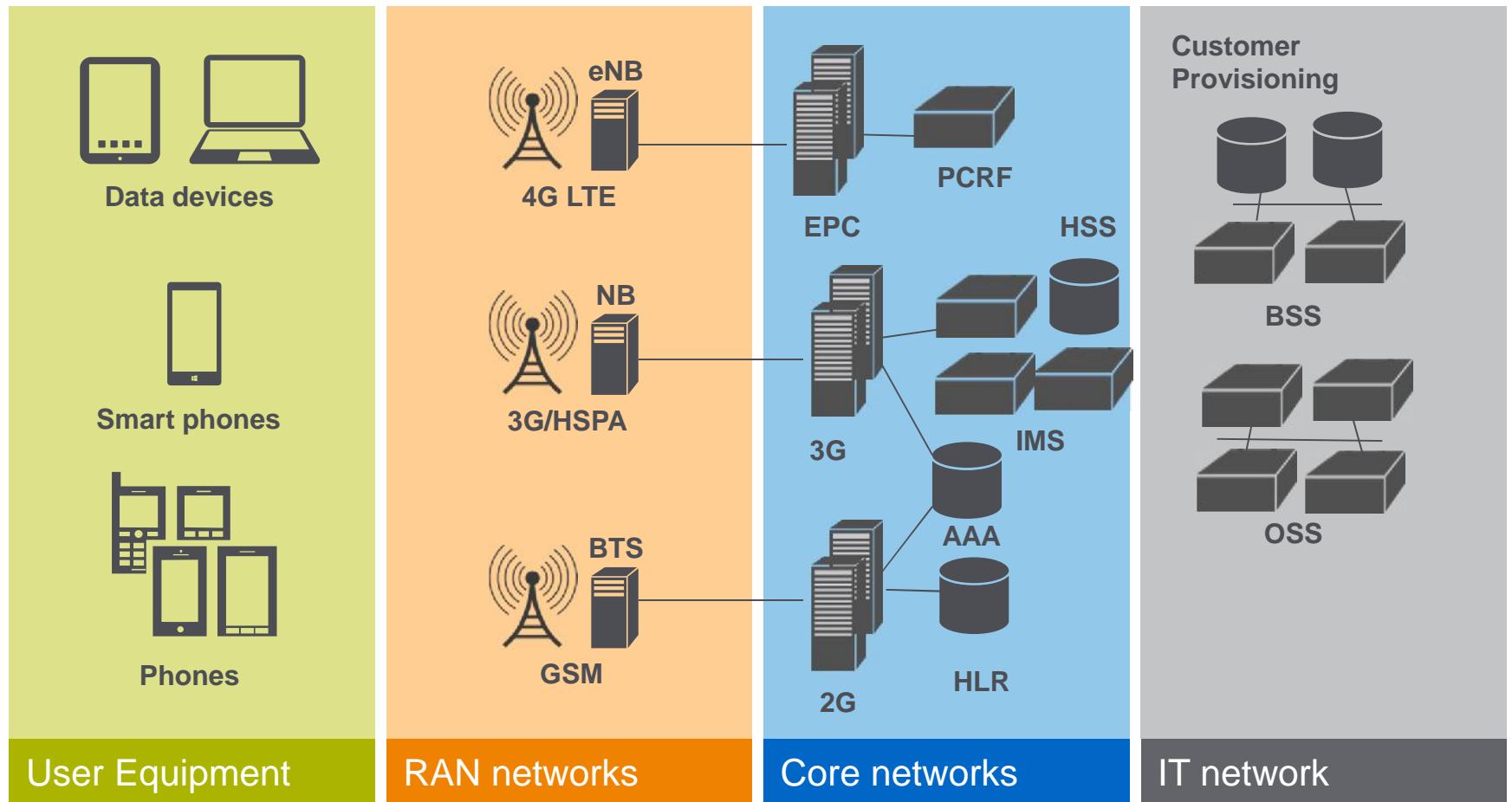
TEST

Amdocs
SERVICES

amdocs

embrace challenge
experience success

Wireless Network Domains



CSP Network Environment

Wireless networks constantly evolving



Complex multiple network topology



Higher data usage, “always on” access



Complex LTE services—increasing load and performance demands



New technology and architectures requiring more agile network



Continuous change, new services—greater demands on network testing processes and resources

The NFV Paradigm Shift

Everything was Known is New Again...

While carriers agree on the advantages for NFV, many are struggling to quantify the development risks, understand the practical migration steps, and how to measure success

Strategic Challenges

- Change management
- What in the NW to virtualize and when?
- Where to begin?
- How to measure success

Architectural Challenges

- New NW devices, techniques, and dependencies
- Service design
- Performance
- Reliability
- Management and orchestration
- Security risks

Operational Challenges

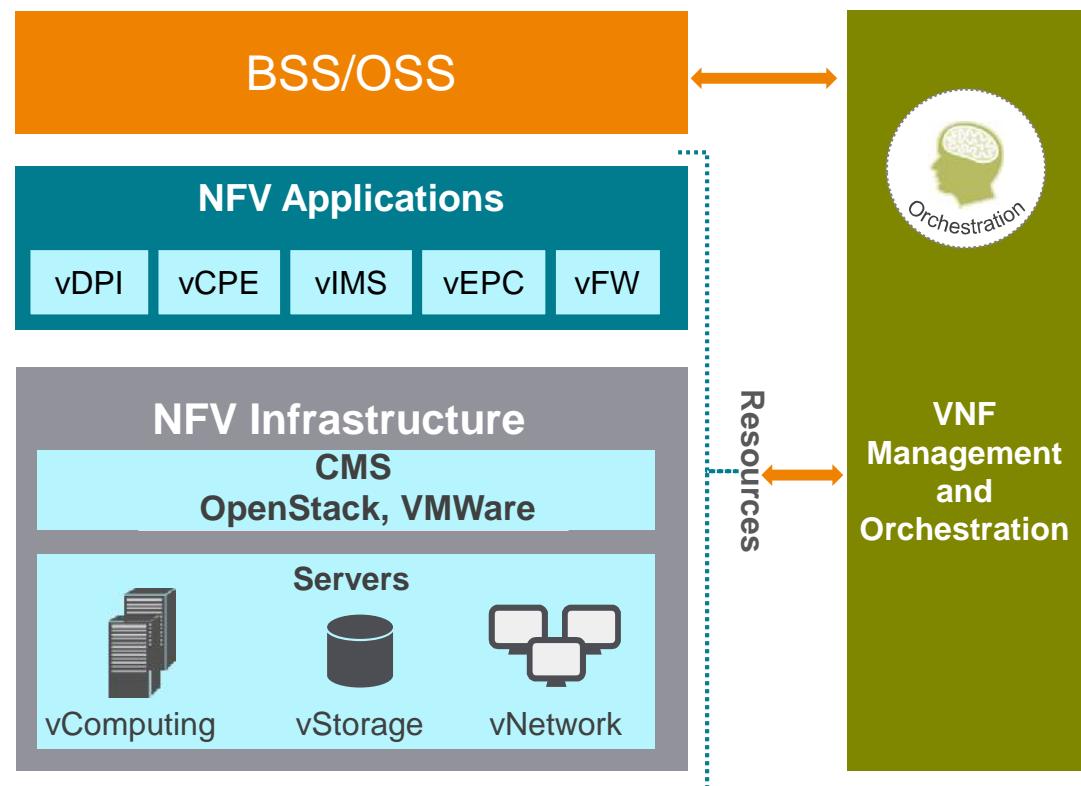
- Managing the complex NFV deployments
- Operational complexity of a virtualized/hybrid carrier networks

Journey to NFV requires change in the way the NW is designed and tested



NFV/SDN Technology Advantages

- Lower equipment costs and reduced power consumption through resource sharing
- Faster time to market by shortening development and testing cycles and utilizing off the shelf HW/SW
- Increased availability of multi-version and multi-tenancy network appliances
- Highly scalability for NW capacity and functionality to meet demands

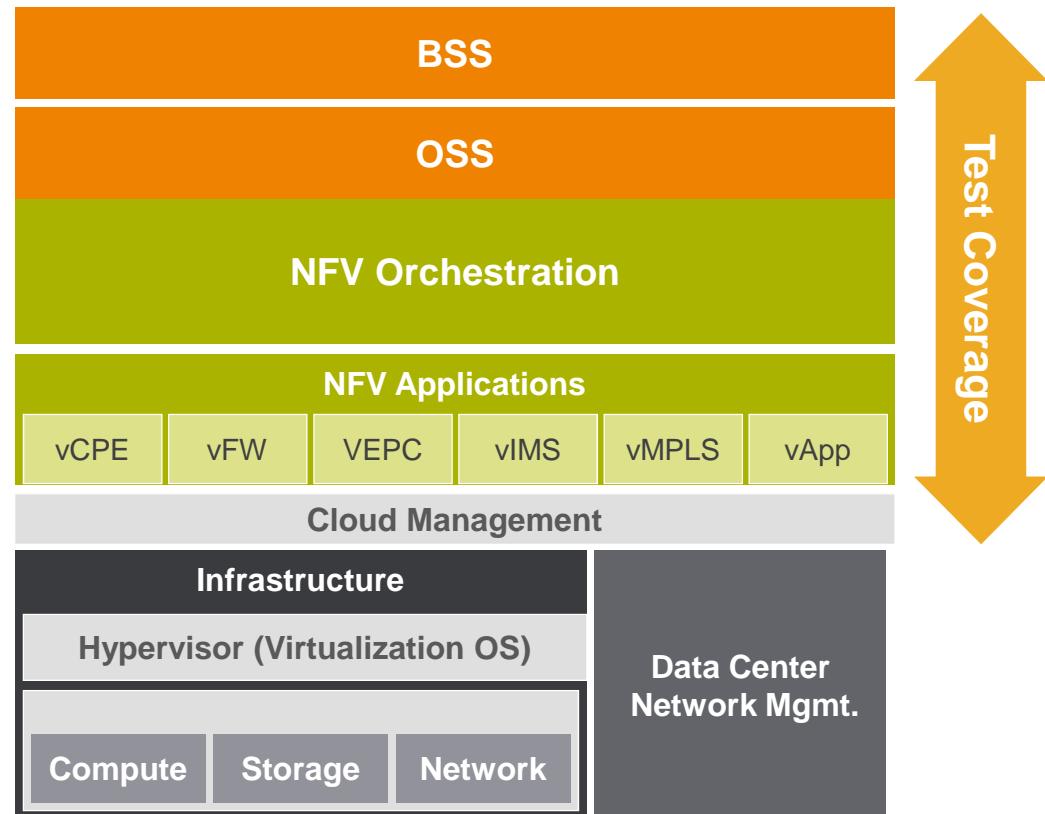


Core networks like EPC/IMS are the prime candidate for NFV development and deployment



NVF/SDN Technology Challenges

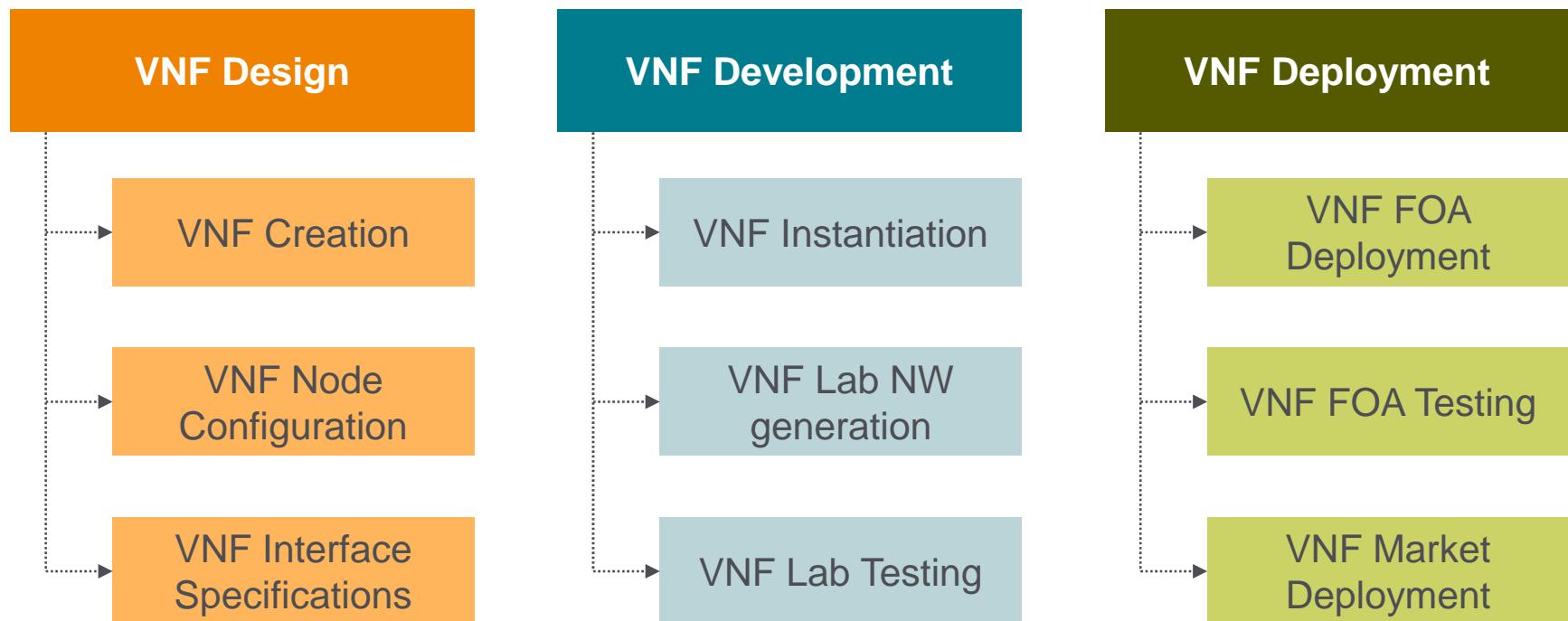
- Integrating multiple virtual appliances from different vendors
- Comprehensive end-to-end testing of virtualized network functions
- Supporting hybrid networks with seamless migration paths to fully-virtualized networks
- Managing and orchestrating numerous virtual network functions, while protecting against attacks and misconfigurations
- Maintaining NW resiliency and reliability from hardware and software failures



For core networks, the seamless interoperability and network operations are critical to CSPs



NFV Design and Development Process



The NFV NW engineering is different than traditional NW engineering methodology, more complex and iterative



NFV Testing and Integration



NFV lab can simulate live production design



VNFs could be from multiple vendors (SGW, PGW, MME, PCRF)



Service orchestration testing to validate VNF functions and configurations with OSS



NW testing to validate interfaces and VNF functionality



NFT testing to validate system performance and load

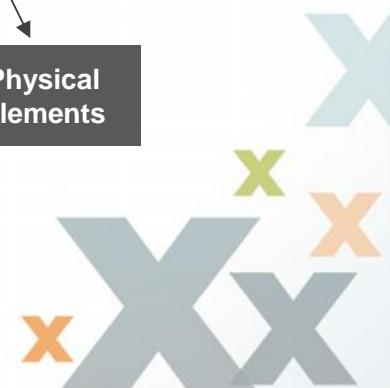
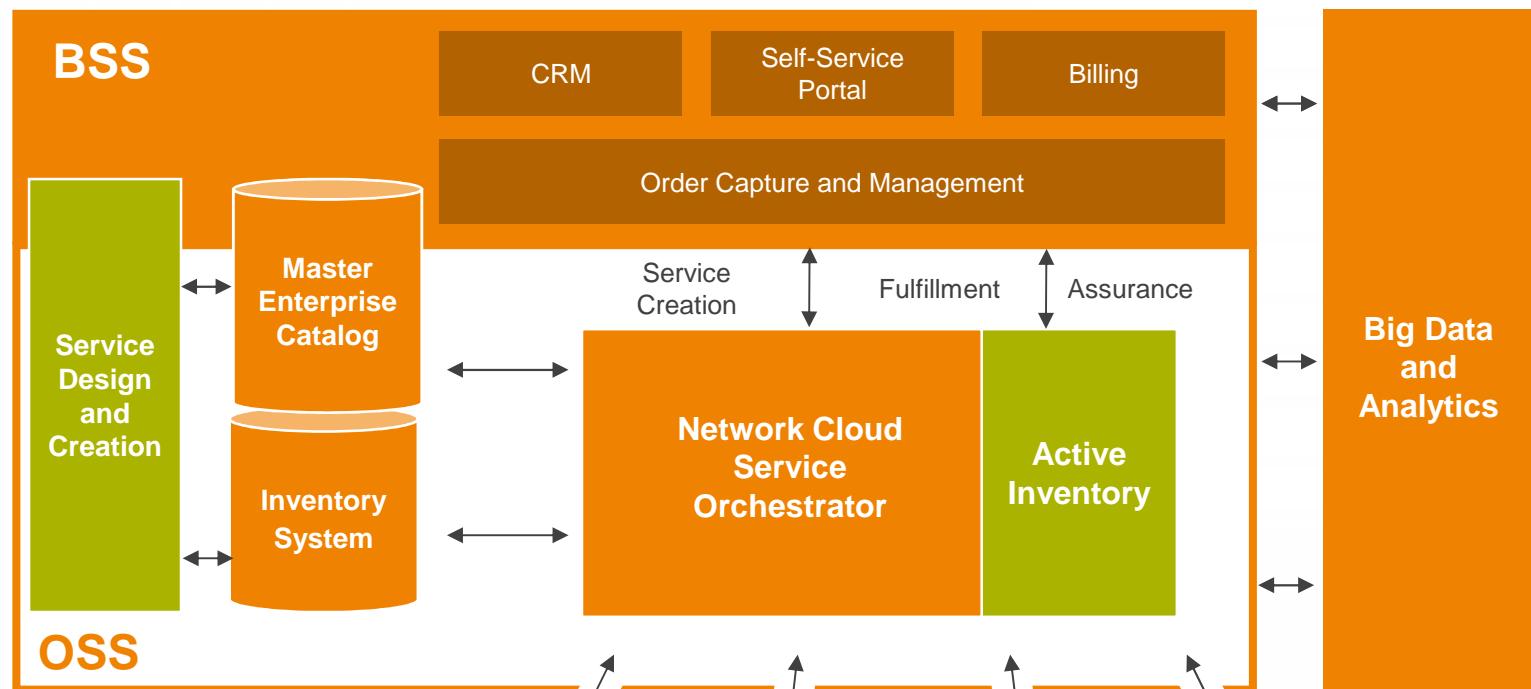


E2E testing to validate E2E functionality and performance of the entire system

The NFV NW testing is different than traditional NW engineering methodology for OSS functions and NW performance: Agile or DevOps is necessary

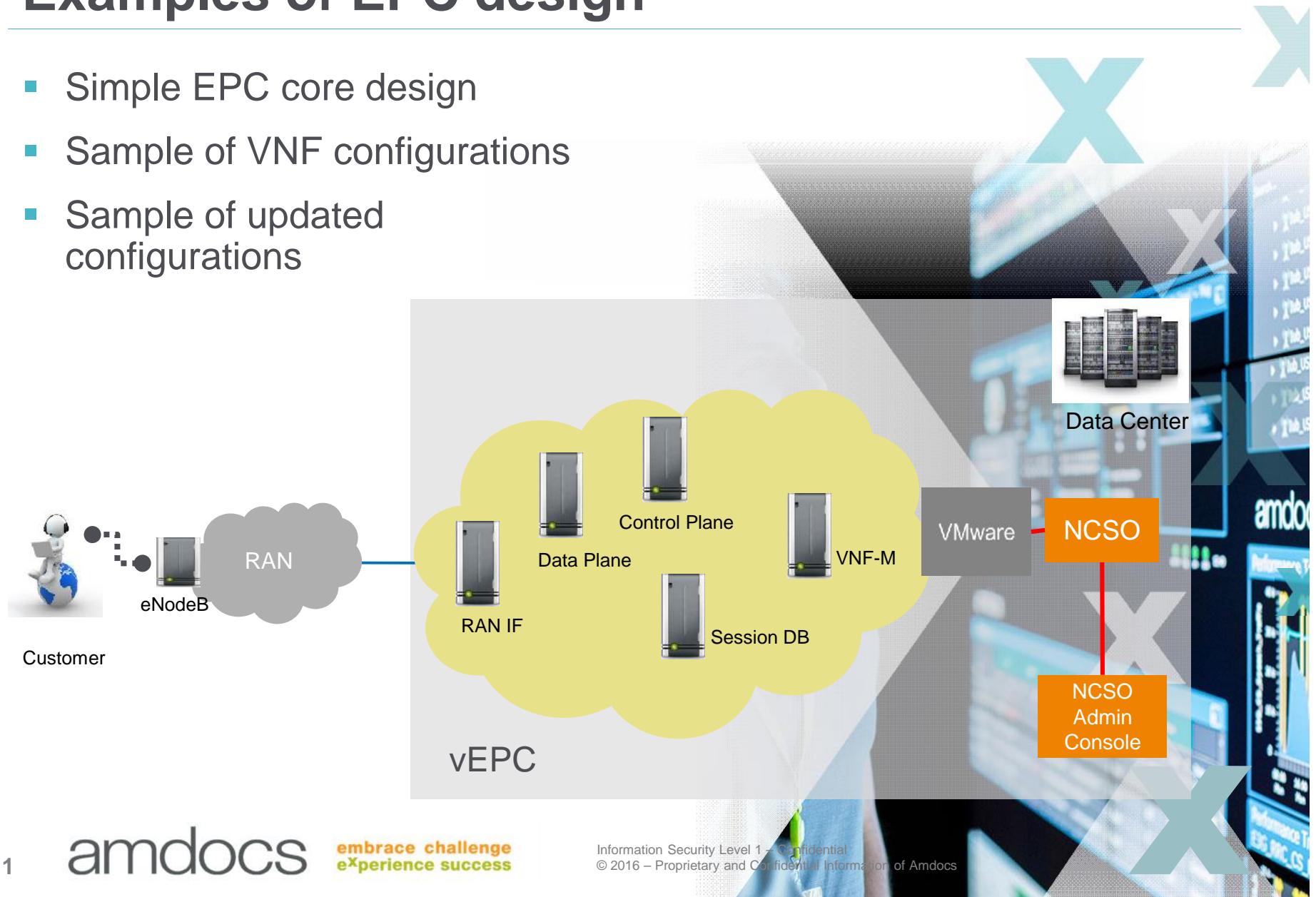


End-to-end NFV Service Offering

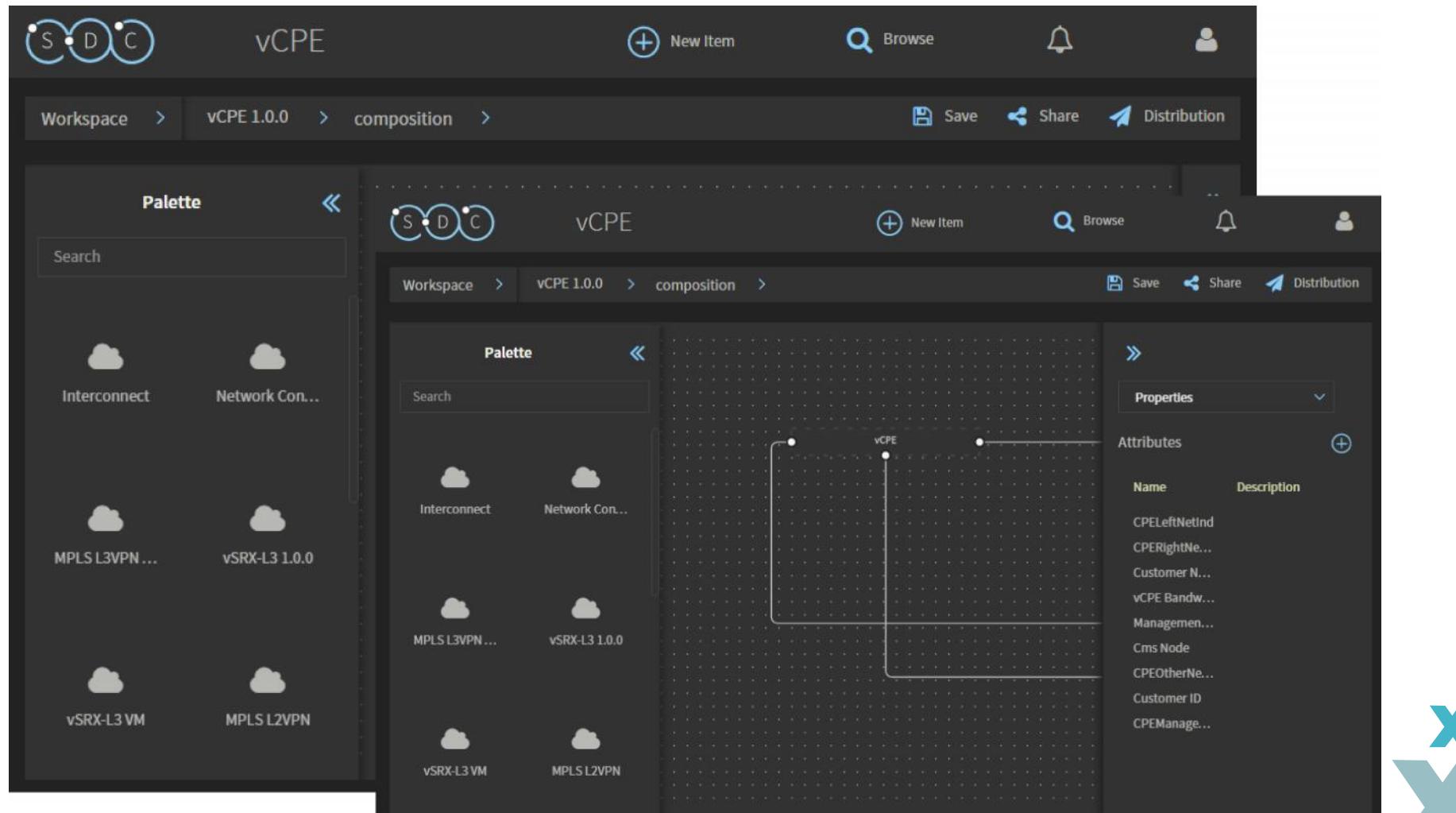


Examples of EPC design

- Simple EPC core design
- Sample of VNF configurations
- Sample of updated configurations



Service Design Tool



vEPC Configuration in Network Orchestrator

NCSO Launch vEPC GR Service 1.0.0

1 Select Service → 2 Parameters → 3 Service Tree → 4 Execution Plan

vEPC Specifications

Max Number Of Subscribers: 50000

Max Number Of Attaches Per Sec*: 200

High Availability Mode*: NCSO

GR Mode*

Launch vEPC GR Service 1.0.0

1 Select Service → 2 Parameters → 3 Service Tree → 4 Execution Plan

Service Network Tree

Primary vDC - Network

Primary RAN Network Ref*

```
graph TD; Root[vEPC Service 1.0.0] --> vEPCCore[vEPC Core 1.0.0]; Root --> MNG[Management Network 1.0.0]; Root --> RAN[RAN Network 1.0.0]; Root --> INT[Internal Network 1.0.0]; Root --> PBN[PEN Network 1.0.0]; vEPCCore --> VDM411[VDM 4.1.1]; vEPCCore --> VDN411[VDN 4.1.1]; vEPCCore --> CDR411[CDR 4.1.1]; vEPCCore --> SERV411[SERV 4.1.1]; vEPCCore --> BH411[BH 4.1.1]; vEPCCore --> CPU411[CPU 4.1.1]; vEPCCore --> UDR411[UDR 4.1.1]; VDM411 --> VMW4111[VMW 4.1.1]; VDM411 --> VMW4112[VMW 4.1.1]; VDN411 --> VDN4111[VDN 4.1.1]; VDN411 --> VDN4112[VDN 4.1.1]; CDR411 --> VCDR4111[VCDR 4.1.1]; CDR411 --> VCDR4112[VCDR 4.1.1]; SERV411 --> VSERV4111[VSERV 4.1.1]; SERV411 --> VSERV4112[VSERV 4.1.1]; BH411 --> VBH4111[VBH 4.1.1]; BH411 --> VBH4112[VBH 4.1.1]; CPU411 --> VCPU4111[VCPU 4.1.1]; CPU411 --> VCPU4112[VCPU 4.1.1]; UDR411 --> VUDR4111[VUDR 4.1.1]; UDR411 --> VUDR4112[VUDR 4.1.1]
```

Back Cancel Re-plan Next

13 amdocs **embrace challenge
experience success**

Information Security Level 1 – Confidential
© 2016 – Proprietary and Confidential Information of Amdocs

Updated vEPC in Network Orchestrator

NCSO vEPC GR Service 1.0.0: Update | Today 01:06 PM - Now (Vodafone)

Overview Service Workflow Topology Parameters Events

Secondary External Network Ref vEPC-POC-HSS-PCRF-Network

vEPC Specifications

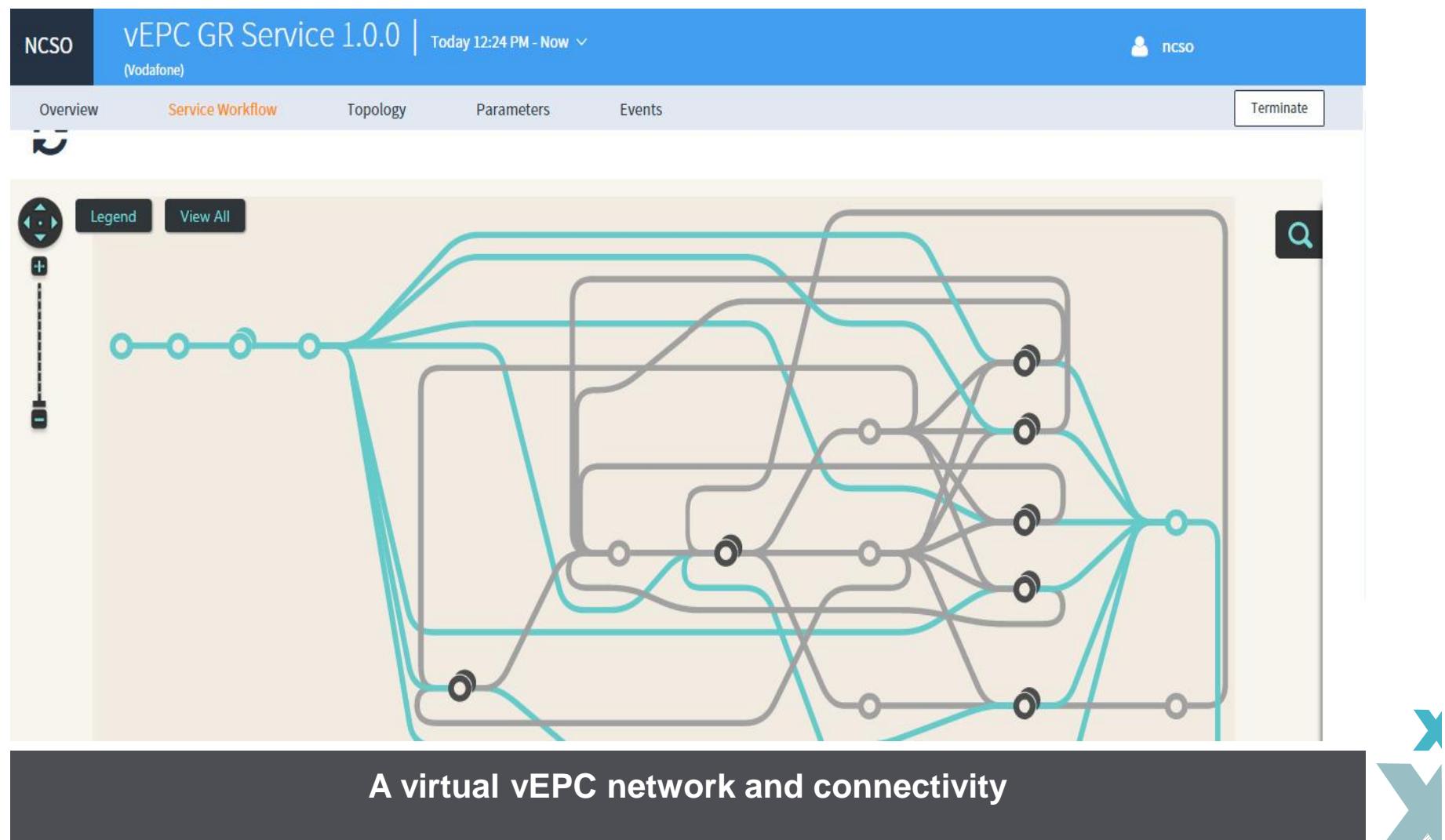
Max Number Of Subscribers: 50000
Max Number Of Attaches Per S: 10000
High Availability Mode*: 1 Update → 2 Impact → 3 Updated service tree → 4 Execution plan
GR Mode*: Service Network Tree

```
graph TD; VCM411[VCM 4.1.1] --> DPE411[DPE 4.1.1]; VCM411 --> UDB411[UDB 4.1.1]; VCM411 --> IN100[Internal Network 1.0.0]; VCM411 --> CPE411[CPE 4.1.1]; DPE411 --> VCMVM411_1[VCM VM 4.1.1]; UDB411 --> VCMVM411_2[VCM VM 4.1.1]; IN100 --> VCMVM411_3[VCM VM 4.1.1]; IN100 --> VCMVM411_4[VCM VM 4.1.1]; CPE411 --> VCMVM411_5[VCM VM 4.1.1]; CPE411 --> VCMVM411_6[VCM VM 4.1.1]
```

14 amdocs **embrace challenge experience success**

Information Security Level 1 – Confidential
© 2016 – Proprietary and Confidential Information of Amdocs

vEPC Virtual Network Graph



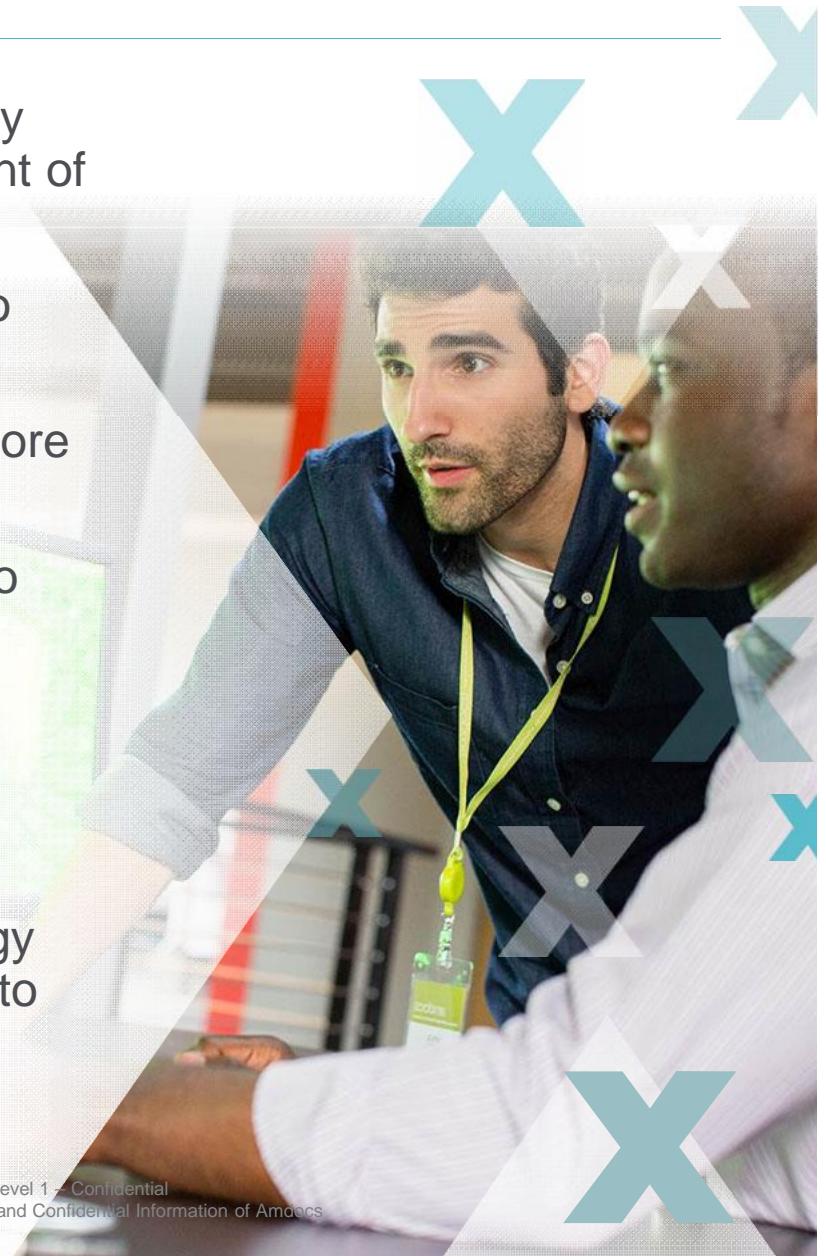
Common Issues with VNF Design

- VNF design phase can take longer to match the production network
- VNF orchestration and configurations are much more complex
- VNF connectivity has to be correctly designed and validated
- VNF deployment in the test lab can simulate the live network
- VNF testing can detect certain defects much sooner: connectivity, protocol, network topology
- VNF testing will require frequent retesting or regression testing after a change in configuration or topology



Summary

- NFV/SDN has many advantages over legacy network to CSPs, enabling faster deployment of new NW functions
- NFV/SDN poses new challenges to CSPs to design, develop and test new NW functions
- NFV technology is much more suitable for core networks such as EPC and IMS cores
- NFV testing will require different approach to test and validate:
 - NFVI layer
 - VNF layer
 - Network Orchestration
 - Network Integration with OSS
- Agile and DevOps development methodology are more suitable for testing NFV/SDN due to higher frequency of NFV deployment



Thank you!

Trinh.vu@amdocs.com

