Network Challenges and Practical Design Consideration for 5G Transformation

Vivek Agarwal, Business Architecture Director vivagarw@cisco.com
Dev Vishwakarma, Principal Architect dvishwak@cisco.com

BRKSPM-3169

Cisco Webex App

Questions?
Use Cisco Webex App to chat
with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click "Join the Discussion"
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated
by the speaker until June 17, 2022.

https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSPM-3169
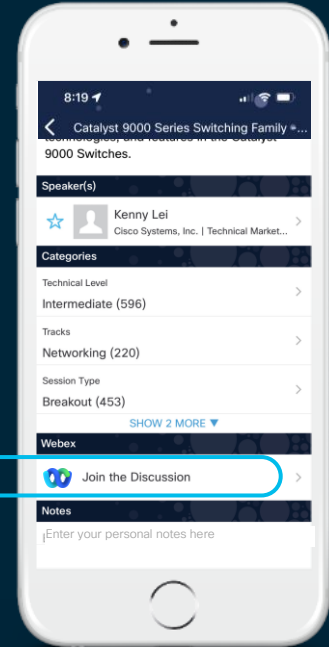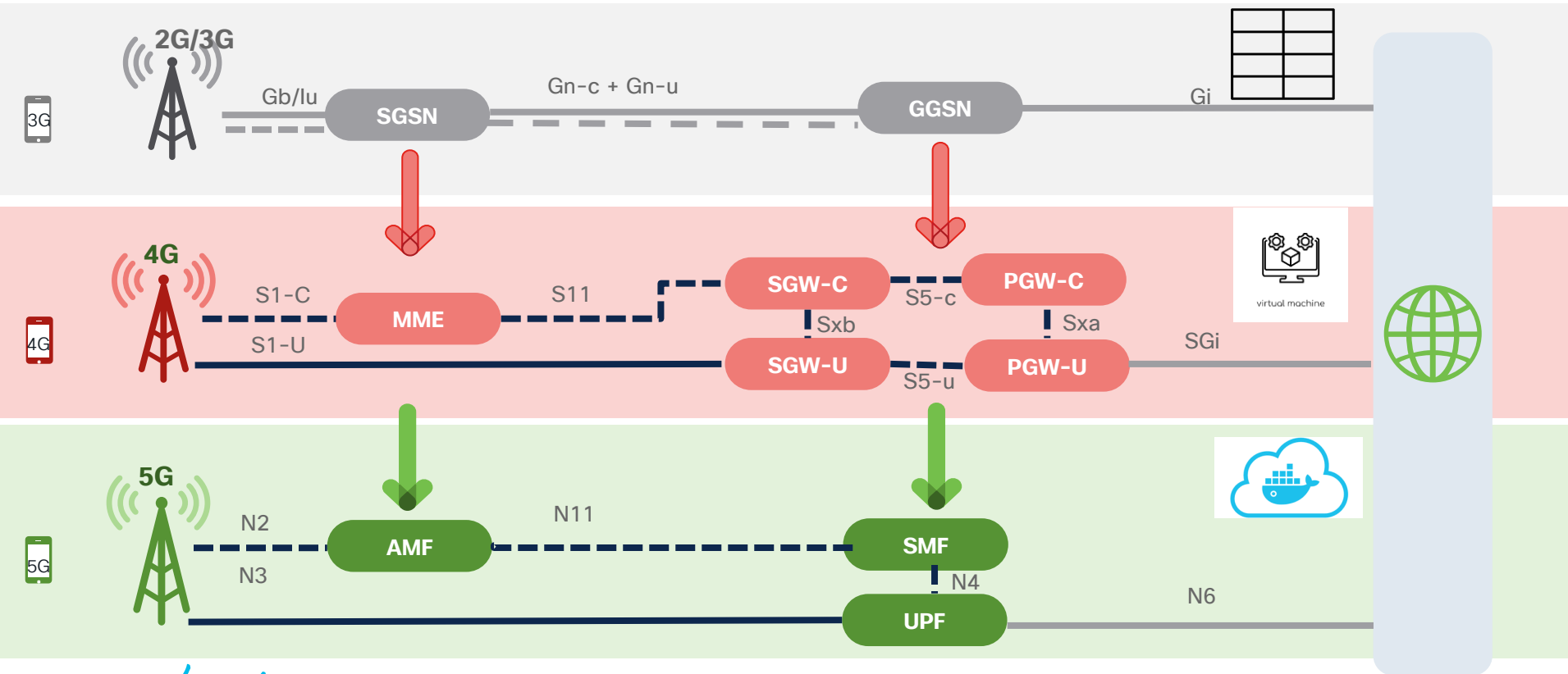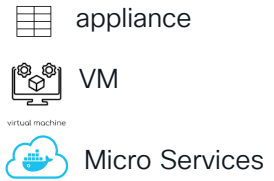
Agenda

- Migration to 5G

- 5G Readiness Considerations

- 5G Security Considerations

- Conclusion

Migration to 5G

Mobile Network Architecture Evolution

3G-4G Co-existence

appliance

VM
virtual machine

Micro Services

2G/3G

3G

Gb/Iu

SGSN

S3

Gn-U

Gn-C

4G

4G

S1-C

MME

S11

SGW-C

S5-c

Sxb

PGW-C + GGSN

Sxa

S1-U

SGW-U

S5-u

PGW-U + GGSN

Sgi+Gi
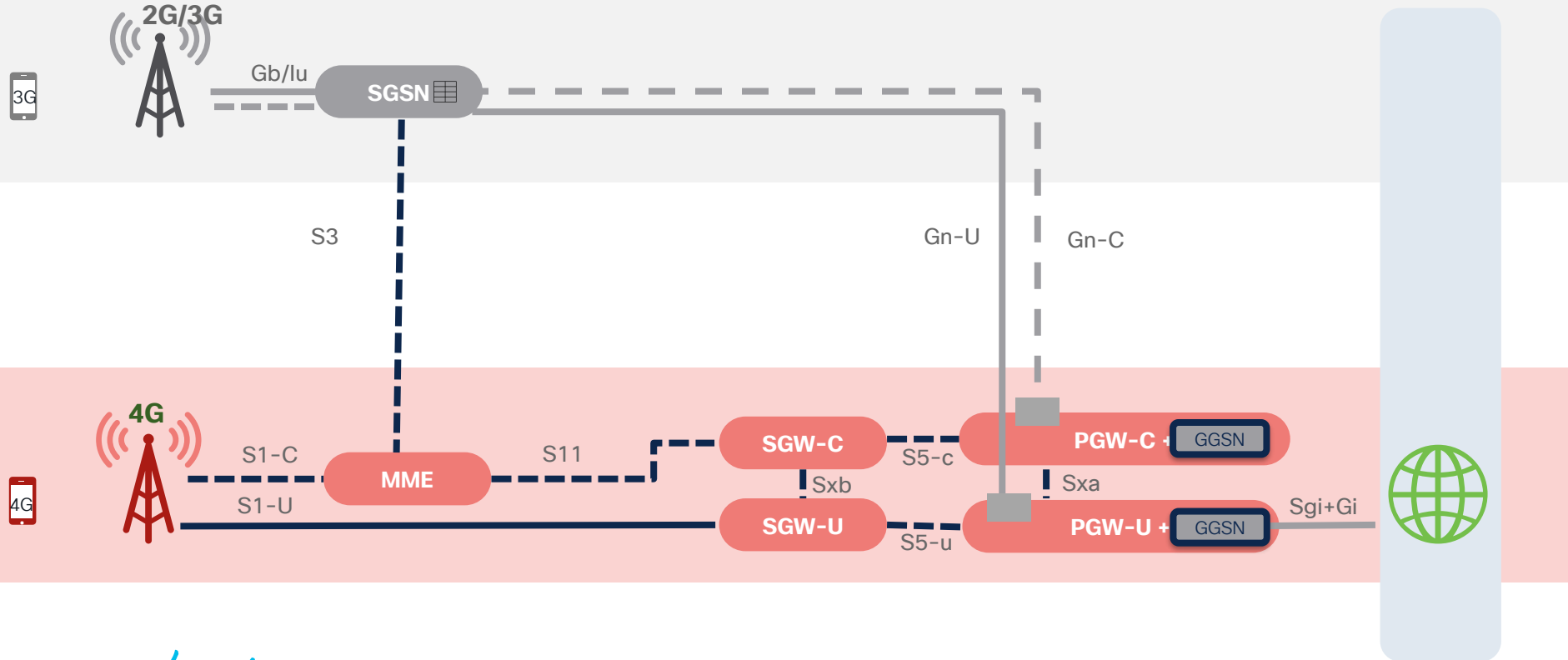
Migration to 5G – NSA – Step1

5G Deployment defines two different options for Migrations from 4G

Option1- The radio part is 5G New Radio (NR) and the core part is 4G Evolved Packet Core (EPC)
(5G Radio + 4G Core = NSA)

Option1- Non-Standalone
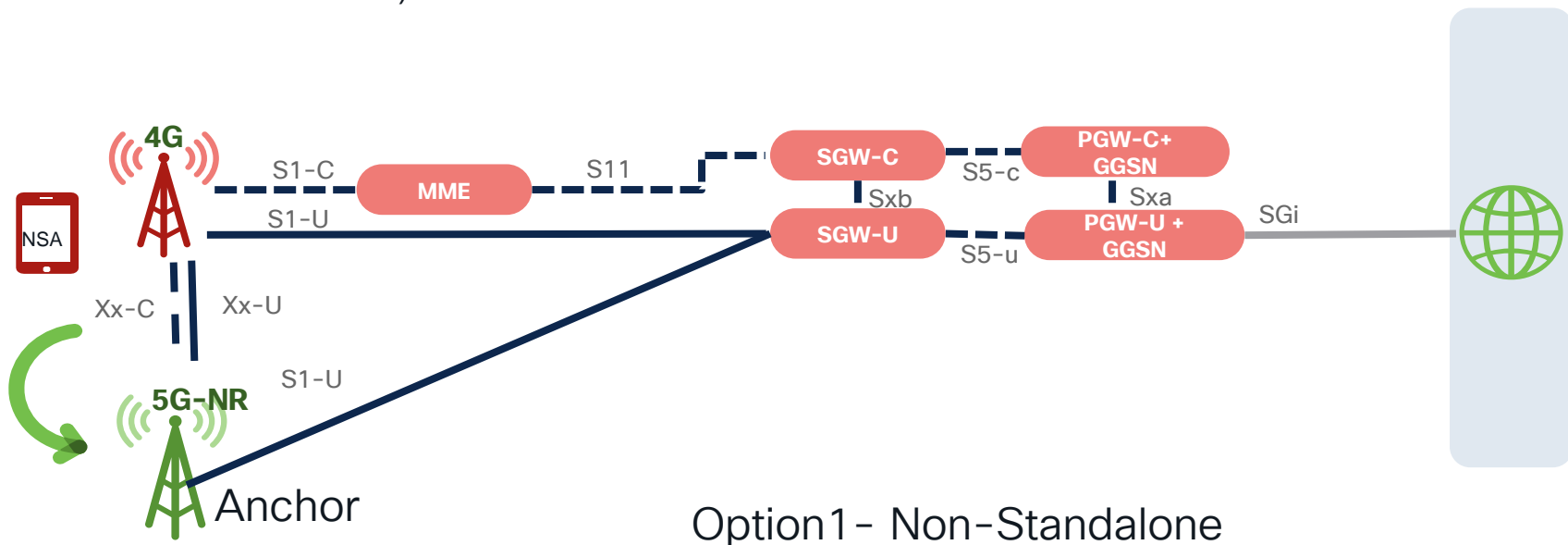
Migration to 5G- SA- Step2

Option2- The radio part is 5G NR and the core part is 5G core; then it is called Stand Alone (5G Radio + 5G Core = SA).

5G Readiness Consideration

5G Deployment Challenges and Lessons learned
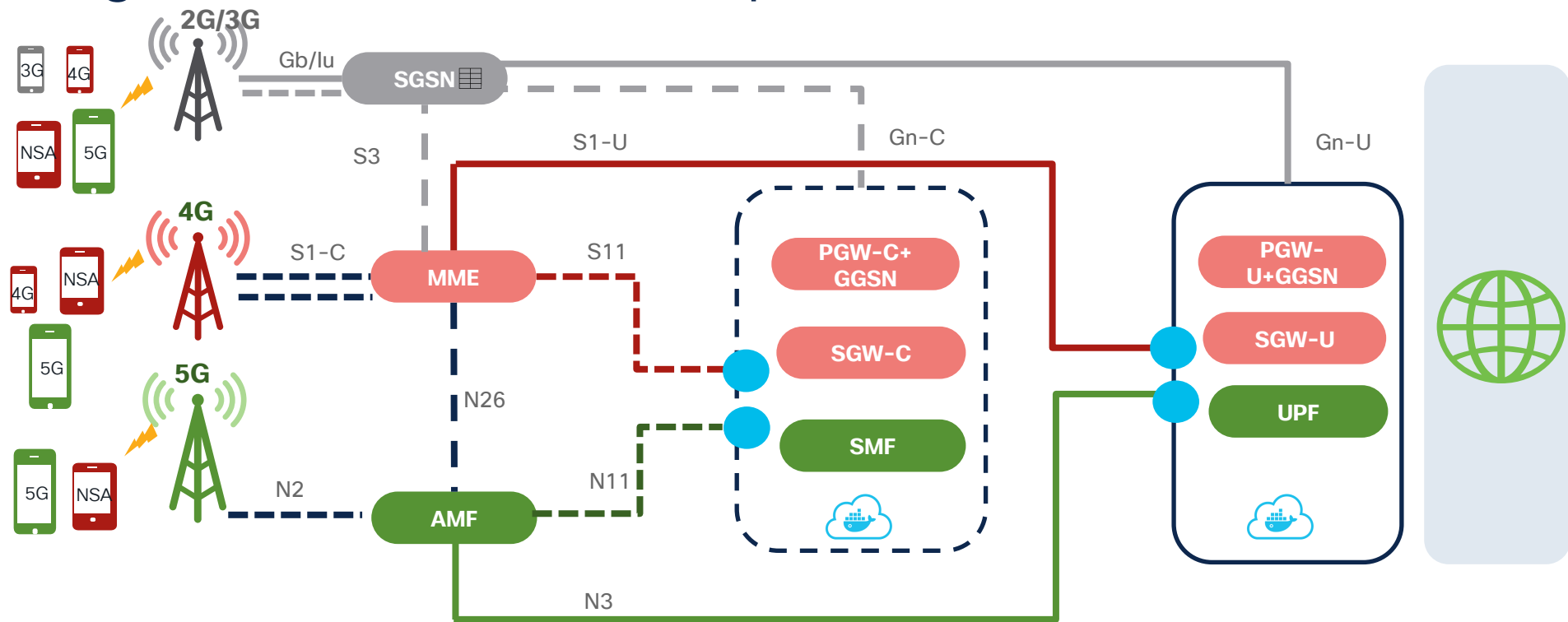
Cloud Infrastructure

- 5G network is typically deployed in cloud native function (CNF) therefore we need major forklift to existing datacenter or interworking between new and old infrastructures

Virtualized RAN

- 5G radio is also virtualized and disaggregated at the edge with a typical cell site is only an antenna, Radio Unit (RU), and an interface function with ethernet capability.

NSA Traffic offload

- Design the 5GC in a manner that provides operators with the flexibility to plan the traffic offloading of NSA UEs based on the capacity and load status on the EPC node

Gateway Selection

- Node selection algorithms in the 4G and 5GNSA network will need enhancements with different combinations of UE subscriptions, APN's used and the UE capabilities to ensure optimized mapping.

N26 support

- Roaming partner networks (domestic roaming partners) May/May not support N26 Interface. This can impact seamless mobility between 5G home and a roamer network

NSA Impact-5G CN

- The implementation of 4G NSA requires EPC core to support dual connectivity, extended bit rate, NR capable gate- way selection, and access restriction capabilities.

Cloud Infrastructure

Evolution

MANO 1	MANO 2	MANO n
VNF1/CNF1	VNF2/CNF2	VNFn/CNFn
NFVI1	NFVI2	NFVIn

- Use Case First approach
- Each VNF/CNF – Own Infra
- Proprietary Software Stacks
- Vertical Clouds
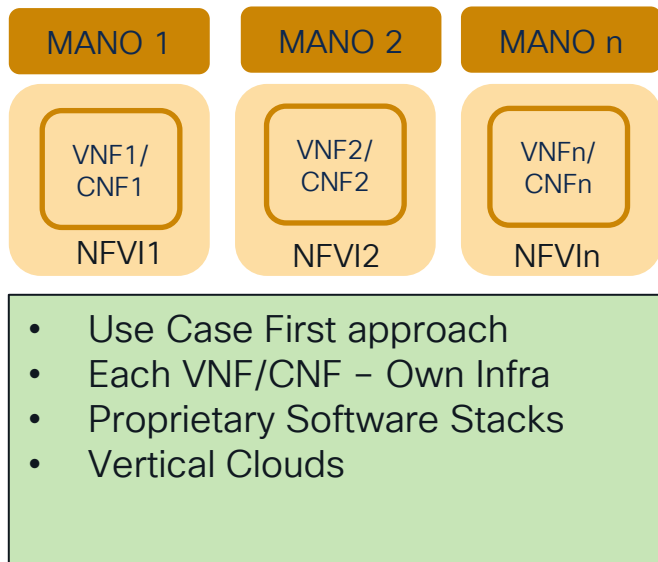
Vertical Solution (Use Case Lead)

Targeted

MANO 1		
VNF1/CNF1	VNF2/CNF2	VNFn/CNFn
	NFVI1	

- All VNF/CNF on single NFV infra
- Infrastructure first approach
- Open API concepts
- Horizontal Clouds
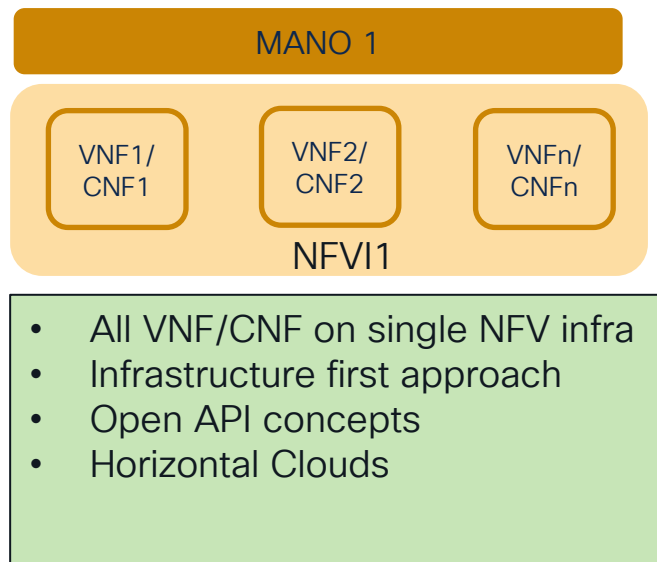
Horizontal Solution (Infrastructure Lead)

Cloud Infrastructure – Hybrid solution

Shared MANO 1	MANO 2	MANO n	Shared MANO p/q

NFVI 1
- VNF1/ CNF1
- VNF2/ CNF2
- VNFm/ CNFm

NFVI 2
- VNF n–1/ CNF n–1
- VNF n /CNF n

NFVI p
- VNF p / CNF p

NFVI q
- VNF q /CNF q
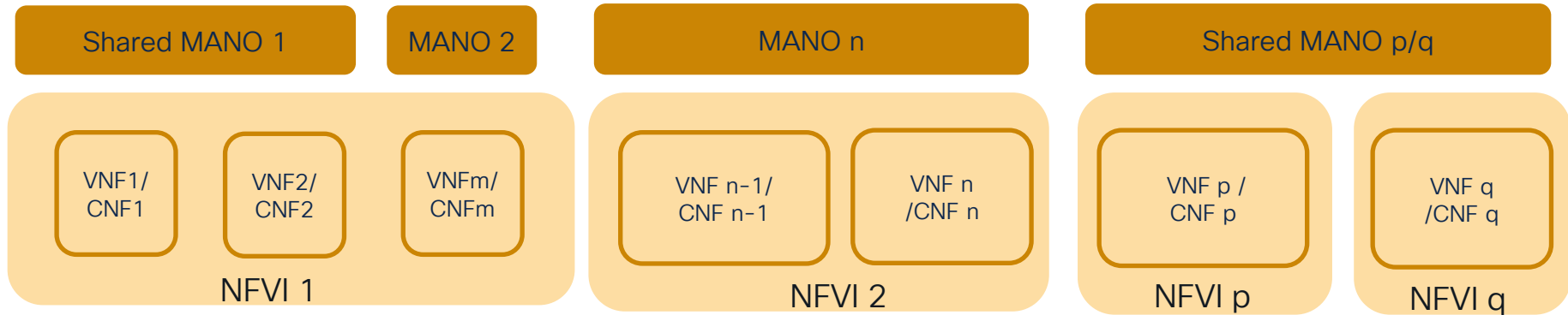
- Most VNF/CNF on single common NFV infra
- Time-to-market approach with plan to migrate to common NFVI in near future
- Open API concept
- Hybrid Clouds
- Most NFs in single NFVI stack initially with converging NFs in near future .
- MANOs can be shared for some NFs with plan to converge to single MANO

Example – Customer Deployment scenario

MANO-1	MANO-2	MANO-2	MANO-3

UDM, AUSF, HSS	UDR	EMS	HDFS	MySQL	Spark	VIA	AMF	SMF	PCF	UPF-KVM

K8s Cluster	K8s Cluster	K8s Cluster
K8s Installer –Openshift	K8s Installer –Rancher	K8s Installer –CNDP

Hardware
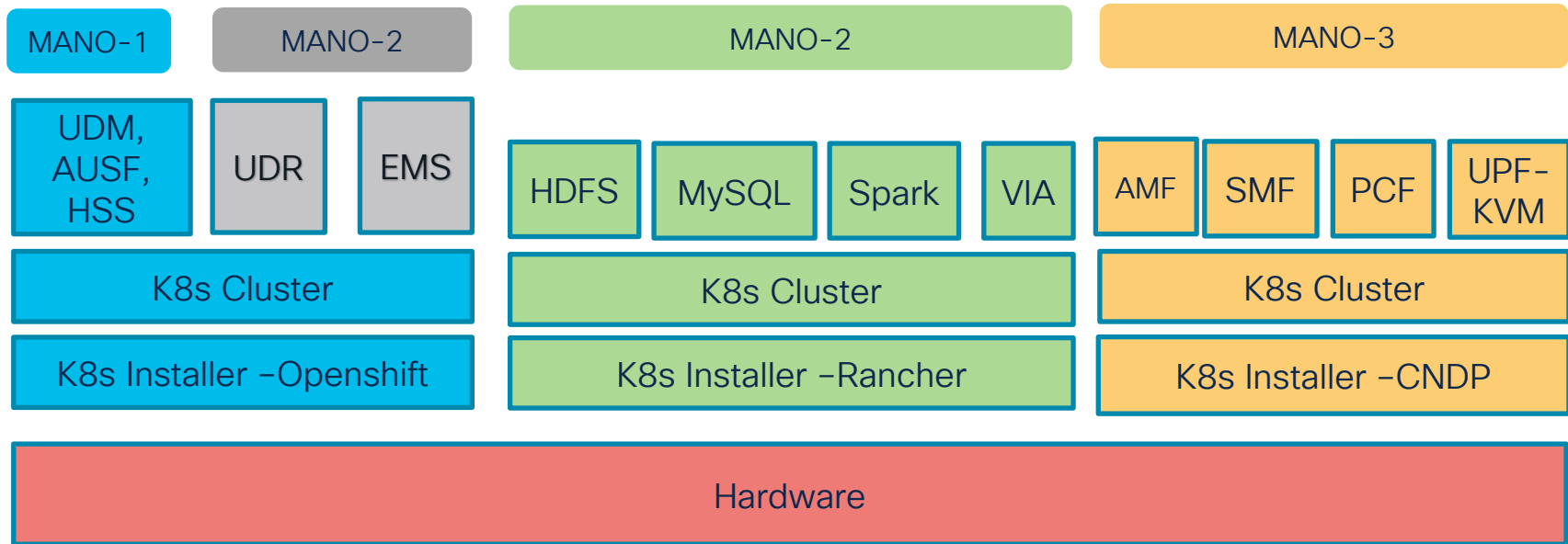
- Don't assume everything can be containerized
- Develop your mano to support kubervert , vm and containerized solution
- Achieve Cost vs Operations balance approach

RAN Architecture Recommendations

Cell-Site   Pre-aggregation   Aggregation   Core

Backhaul   5GC

eCPRI-Fronthaul   Midhaul   Backhaul
RU   vDU   vCU   5GC

eCPRI-Fronthaul   vCU
vDU   Backhaul   5GC
RU

Hybrid
cell-site   eCPRI-Fronthaul   UPF   Backhaul   5GC
RU   vCU

vDU   vRouter
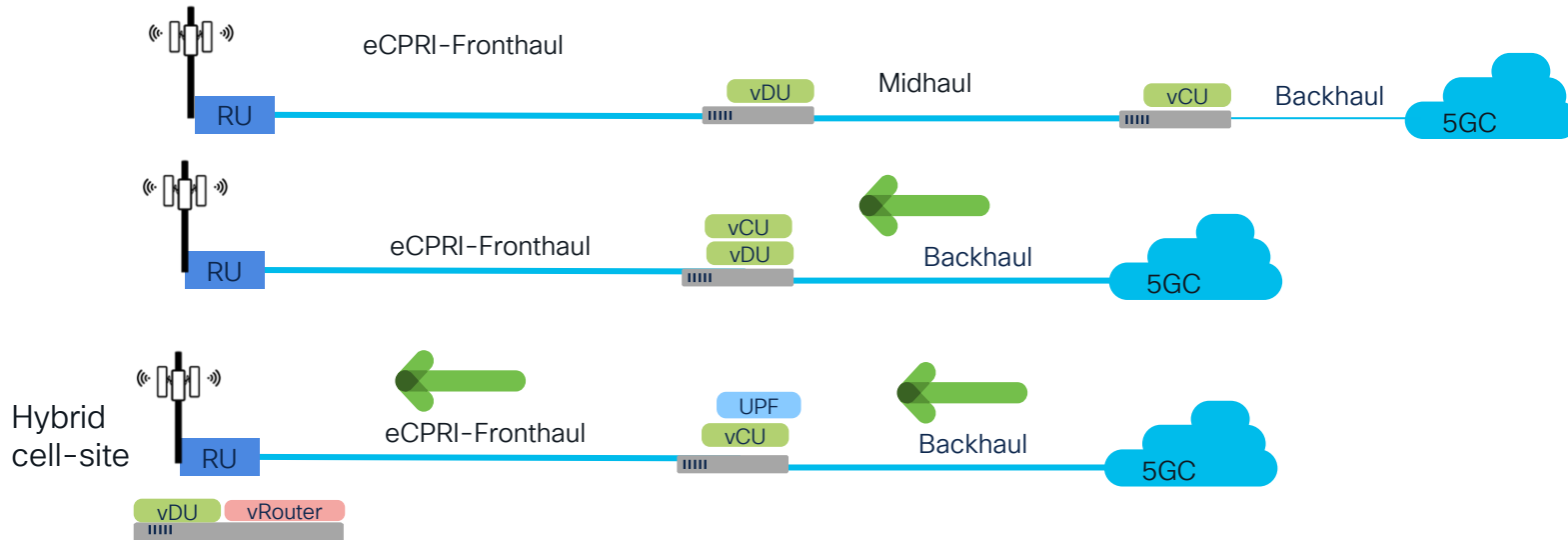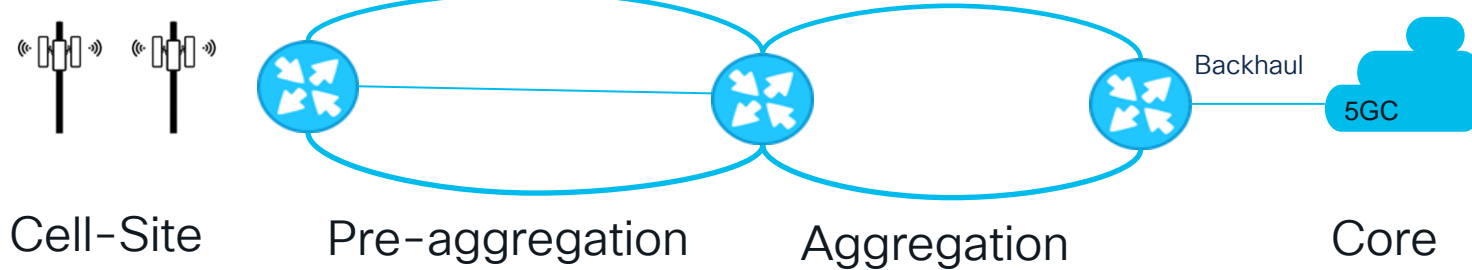
Hybrid Cell Site learnings

- Zero-touch server onboarding and operations are one of the key requirements for a hybrid cell site

- vDU to vRouter communication has to be agreed upon by both vendors

- ZTP of vRouter orchestration has to be stitched with vDU and Kubernetes Orchestration

- Packet size between vDU and vRouter impacts the total bandwidth requirements

- Resource allocation of the vRouter and vDU has to be planned as space and power at cell sites are limited.

NSA Traffic offload

Standard Architecture

4G UE → 4G EPC (PGW-C, PGW-U)

4G NSA UE — 5G NSA UE routes traffic to EPC

5G UE → 5GC Network slice A (PGW-C+SMF, PGW-U+SMF)

5GC Network slice B (PGW-C+SMF, PGW-U+SMF)

Optimized Architecture

4G UE → 4G EPC (PGW-C, PGW-U) — Overloaded EPC Core

4G NSA UE — 5G NSA UE Loadbalances traffic

5G UE → 5GC Network slice A (PGW-C+SMF, PGW-U+SMF)

5GC Network slice B (PGW-C+SMF, PGW-U+SMF)
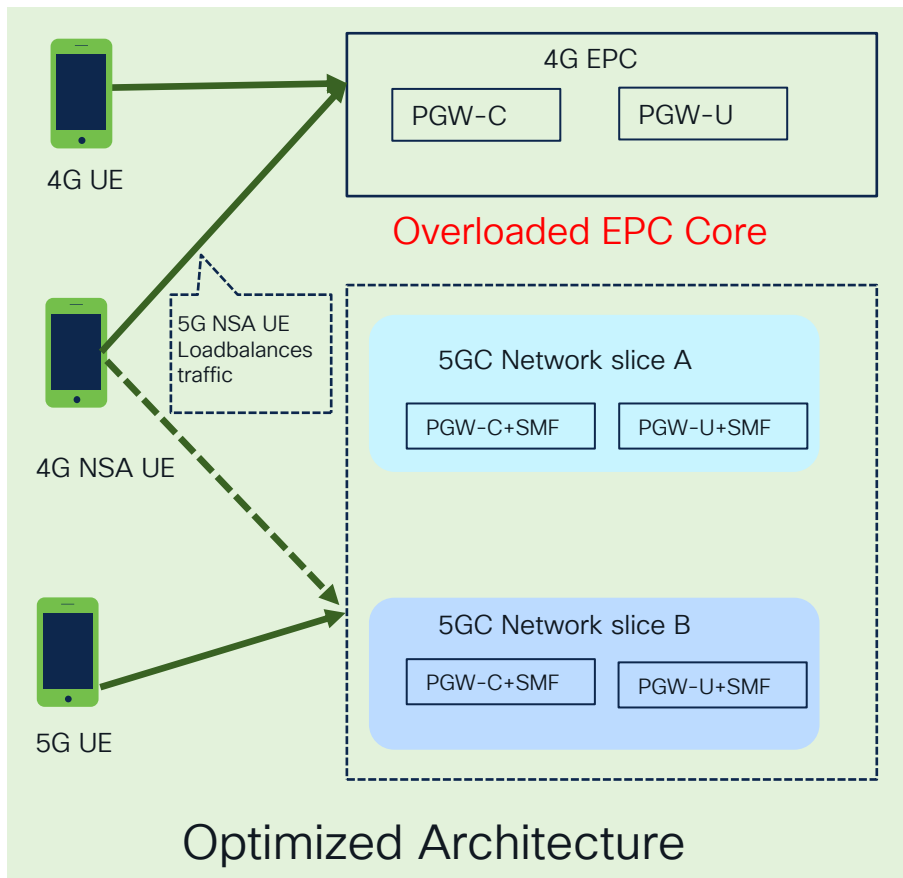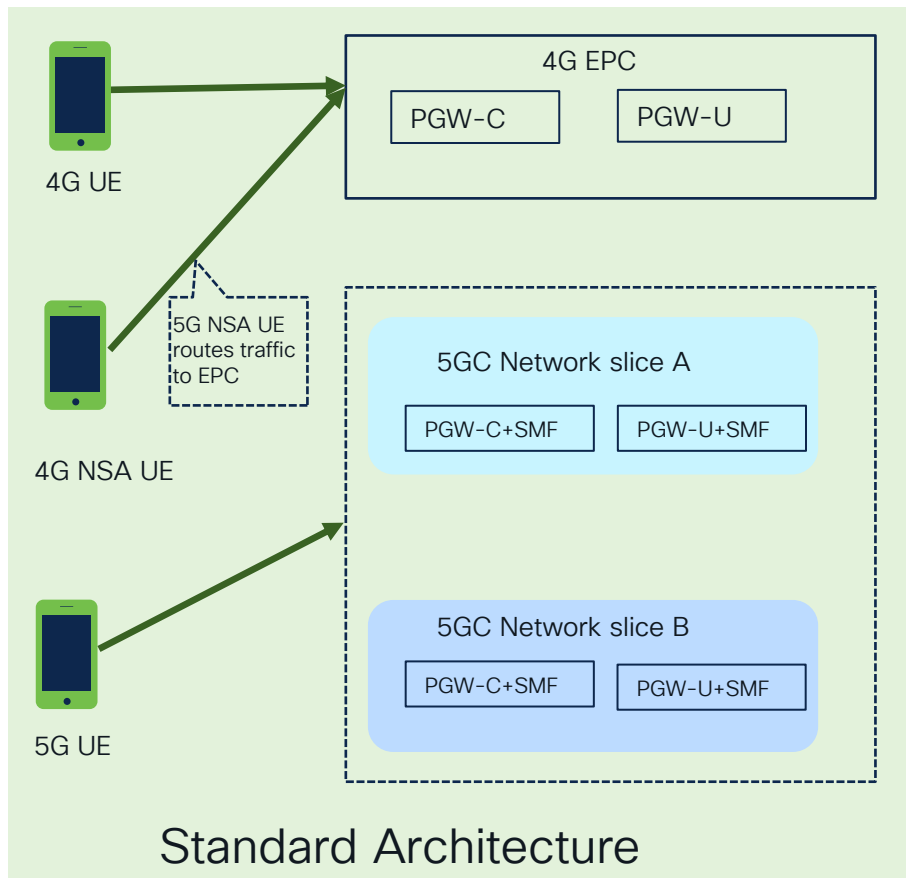
Gateway Node Selection

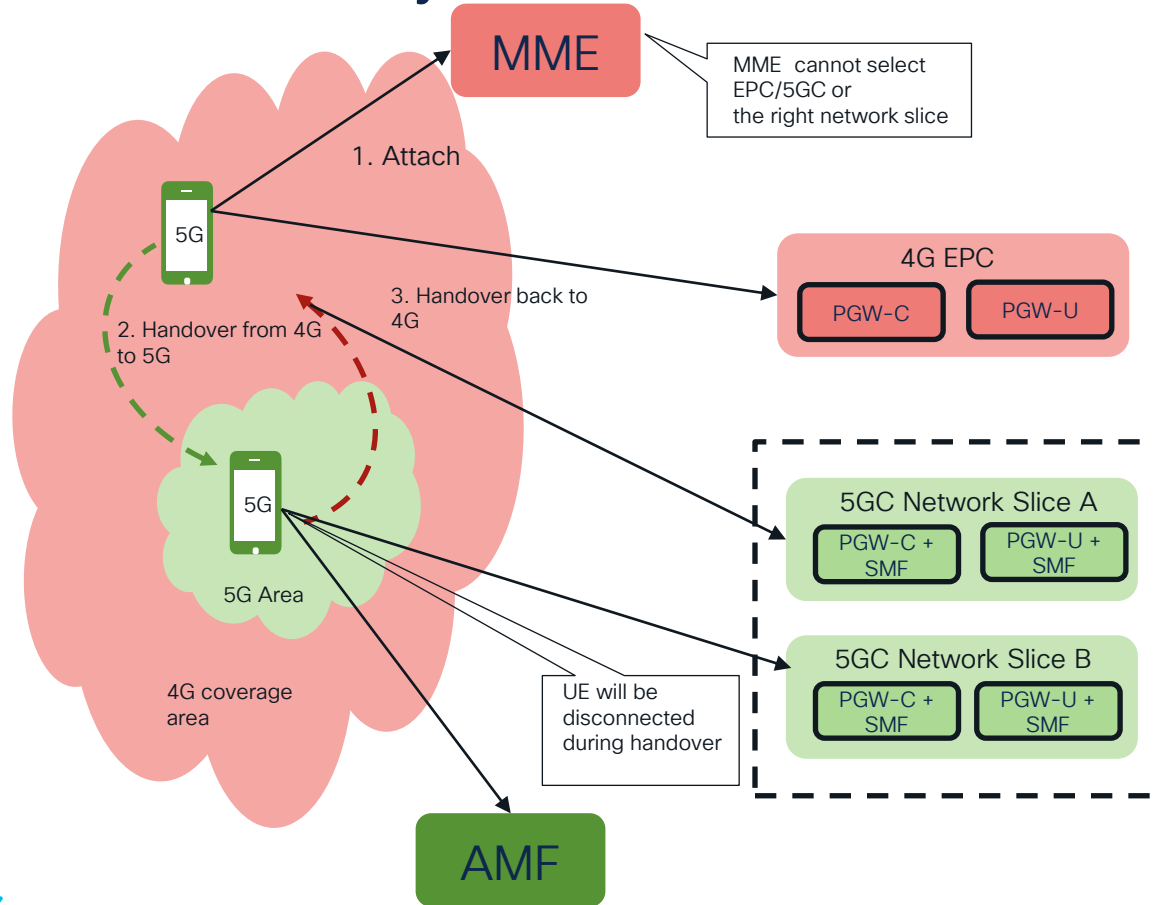| Scenario	UE 5GC NAS Capability	Core-Network-Restrictions (ULA)	Interworking-5GS APN-Configuration	MME Policy	DNS Request	5GSIWKI	5GCNRS	5GCNRI	PGW or SMF
	From UE	From HSS		Local	Local policy	On S11			PGW/SMF
1-4	Yes or No	5GC not allowed	SUBSCRIBED or NOT SUBSCRIBED	No	PGW	0	1	0	PGW
5	Yes	5GC allowed	SUBSCRIBED	No	SMF (nc-smf)	1	1	1	SMF
6	Yes	5GC allowed	NOT SUBSCRIBED	Operator Policy	SMF or PGW	0	1	0	SMF or PGW
7	No	5GC allowed	SUBSCRIBED	Operator Policy	SMF (nc-smf)	0	1	1	SMF
8	No	5GC allowed	NOT SUBSCRIBED	Operator Policy	SMF or PGW	0	1	0	SMF or PGW

Enhanced Gateway node selection- Challenge

MME

MME cannot select EPC/5GC or the right network slice

1. Attach

3. Handover back to 4G

2. Handover from 4G to 5G

5G

5G

5G Area

4G coverage area

4G EPC

PGW-C   PGW-U

5GC Network Slice A

PGW-C + SMF   PGW-U + SMF

5GC Network Slice B

PGW-C + SMF   PGW-U + SMF

UE will be disconnected during handover

AMF

Enhanced Gateway node selection- Solution

MME

MME selects a proper network and
the right network slice

1. Attach

3. Handover back to 4G

2. Handover
from 4G to 5G

5G Area

4G coverage area

4G EPC

PGW-C   PGW-U

5GC Network Slice A

PGW-C + SMF   PGW-U + SMF

5GC Network Slice B

PGW-C + SMF   PGW-U + SMF

AMF
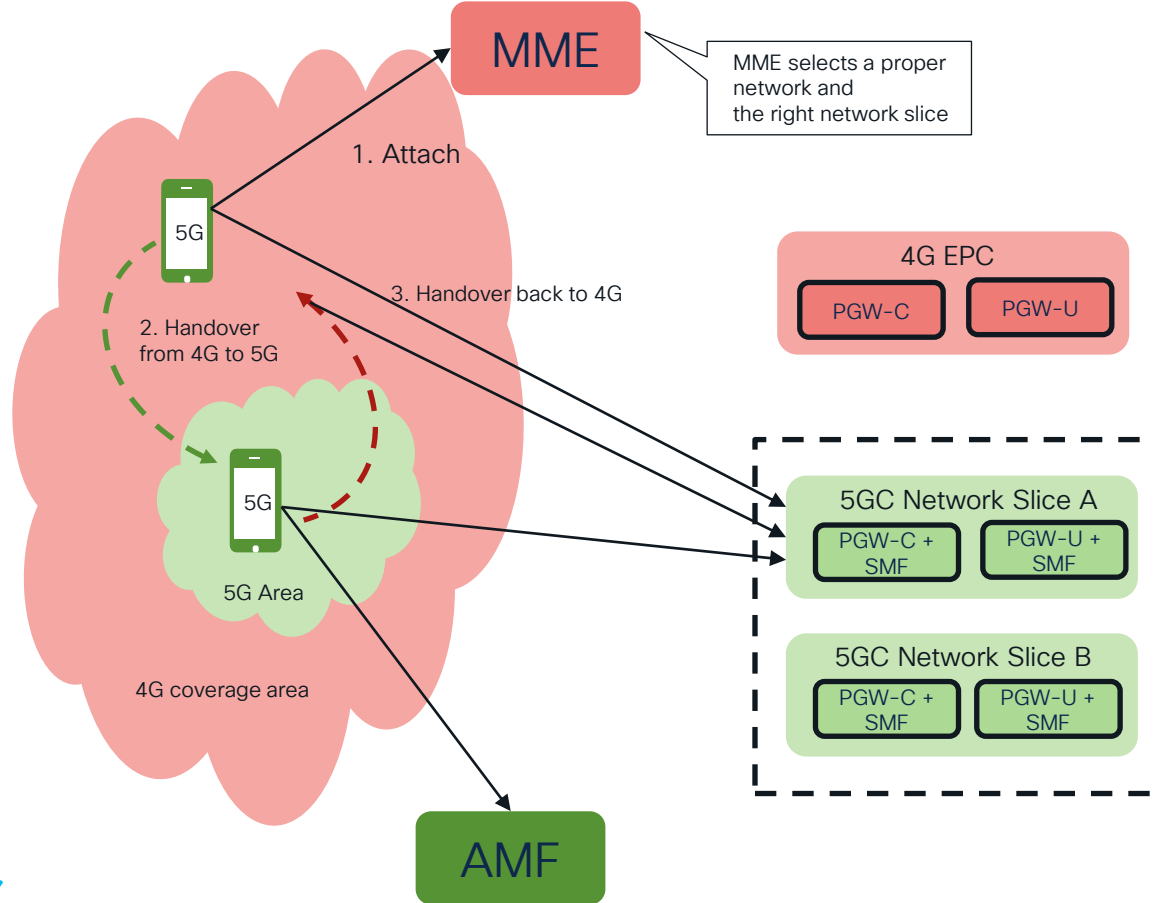
Enhanced Gateway Node Selection

UE Capability	UE Subscription	APN Selected by UE	SAEGW Selection logic in MME
5G SA Capable	5G Subscription	4G data apn	SAEGW in EPC
		5G data apn	SGW in EPC , PGW+ SMF in 5GC
5G SA Capable	4G Subscription	4G data apn	SAEGW in EPC
		5G data apn	Attach/TAU Rejected
4G Capable	5G Subscription	4G data apn	SAEGW in EPC
		5G data apn	SGW in EPC , PGW+ SMF in 5GC
4G Capable	4G Subscription	4G data apn	SAEGW in EPC
		5G data apn	Attach/TAU Rejected

Enhanced Gateway Node Selection

For 4G and NSA users using 4GAPN, the selection network selection can be as before

In case 5G UE + 5G Subscriber: the 5G PGW-c + SMF combo node will be selected to ensure seamless handover

DNS

HSS

PCRF

IMS

MME

S6a

S11

SGW-C

S5-C

Gx

PGW-C

for 4G-DATA-APN

4G / NSA/ SA UE

S1-MME

4G RAN

eNB

S1-U

SGW-U

S5-U

Sx

PGW-U

N26

5G SA RAN

AUSF

UDR

UDM

NSSF

PCF

Rx

N13

N8

NRF

CHF

N7

5G SA UE

AMF

N2

N12

N11

PGW-C + SMF

for 5G-DATA-APN

GNB

N3
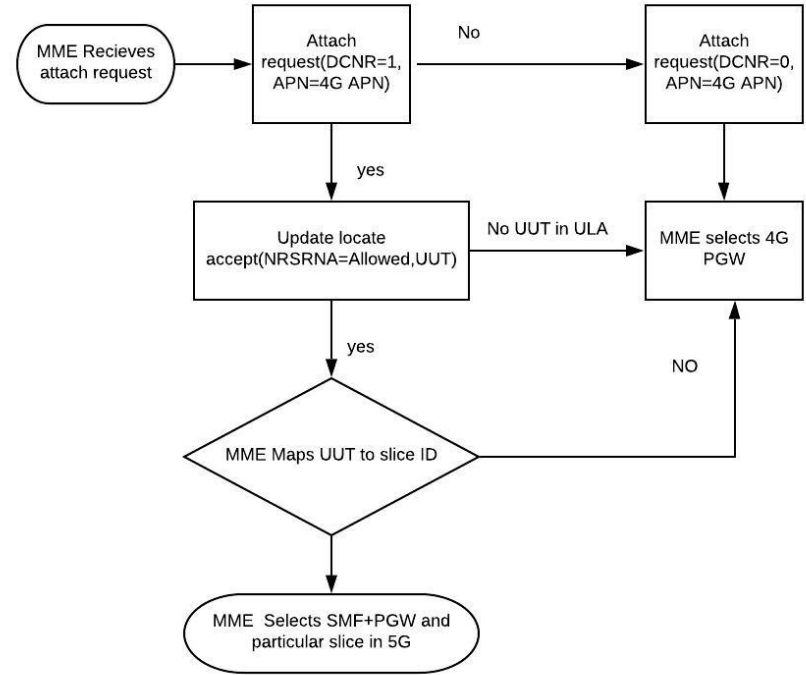
N4

PGW-U + UPF
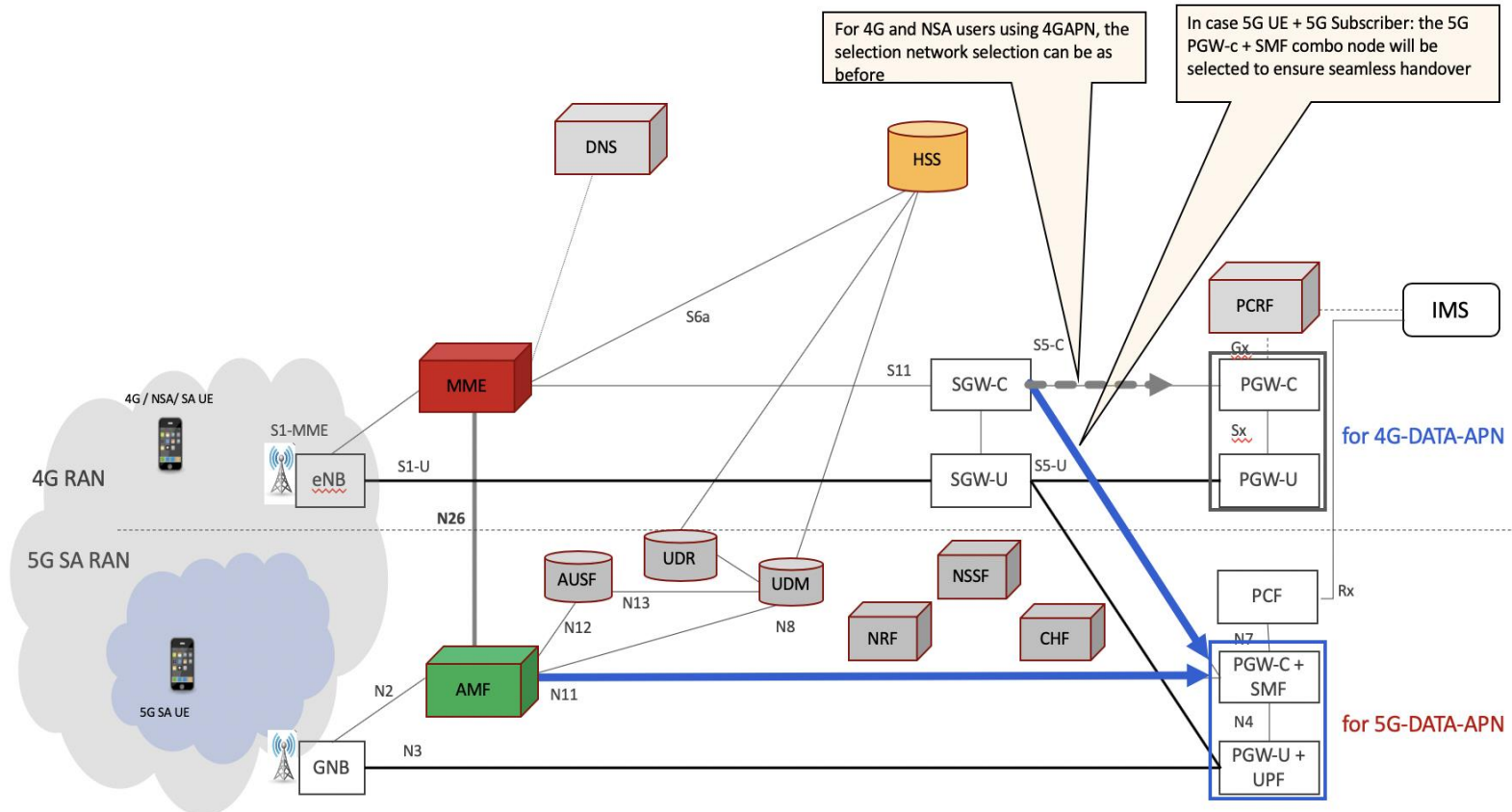
Enhanced gateway node selection – Multiple slice
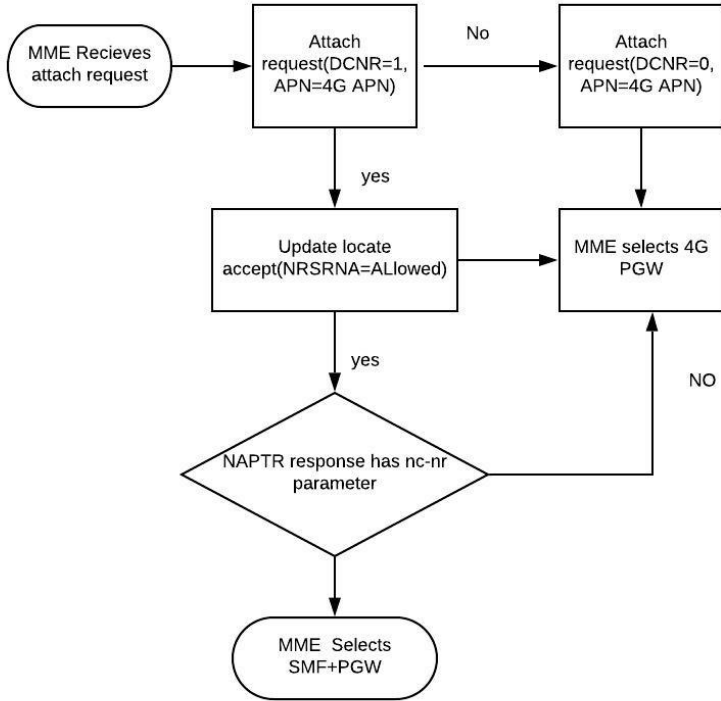
Gateway Selection using nc-nr with one slice in 5G

Gateway Selection using UUT mapping with multiple slices in 5G
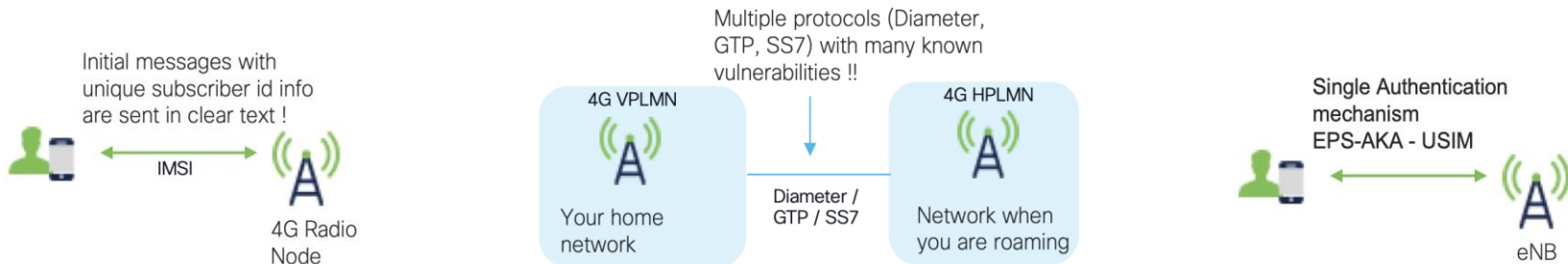Defensive publication

NSA Impact on 5G Core

Features	RAN	MME	SGSN	HSS	SGW-C PGW-C	SGW-U PGW-U	PCRF	CHG	DNS	SUPPORT
Subscription control	✓	✓	✓	✓						Restrict subscriber from NR access based on subscription
5G Icon display	✓	✓		✓						Display of 5G icon
Dual connectivity mobility support	✓	✓								Allow / reject the NR addition
Max bit rate value	✓	✓		✓	✓	✓	✓			Encoding and processing of extended MBR/GBR values
Voice support	✓									Prevent voice to move to NR
Security impact	✓	✓								5G security capabilities
SPGW selection		✓	✓		✓	✓			✓	S/PGW which can support NR high data rate
NR usage reporting	✓	✓			✓			✓		UE usage of NR reporting
Low latency support	✓				✓		✓			NEW QCI value of NR support

Security Considerations

3GPP Security Evolution

4G Networks

Initial messages with unique subscriber id info are sent in clear text !

IMSI

4G Radio Node

Multiple protocols (Diameter, GTP, SS7) with many known vulnerabilities !!

4G VPLMN
Your home network

Diameter / GTP / SS7

4G HPLMN
Network when you are roaming

Single Authentication mechanism
EPS-AKA - USIM

eNB

5G Networks

Initial messages with unique subscriber id info are now encrypted in 5G !

SUPI   SUCI

5G Radio Node

APIs are used in 5G with a defined network function called Secure edge Protection Proxy (SEPP)

5G VPLMN
Your home network

SEPP   http/2   SEPP

5G HPLMN
Network when you are roaming

5G allows multiple Authentication mechanism
• 5G-AKA - USIM
• EAP-AKA' - USIM
• EAP-TLS – USIM / Non-USIM

eNB

Practical 5G security considerations

Zero Trust

- Data at rest & in motion must be encrypted (TLS 1.2, SSHv2, NETCONF over TLS)
- MFA for management plane
- Only applications can access and transfer data
- All data access and transfer must be logged

Threat Protection

- Which SBIs to protect?

  (N1/N2/N3/N4/N5/N6)

- And how much protection is enough?
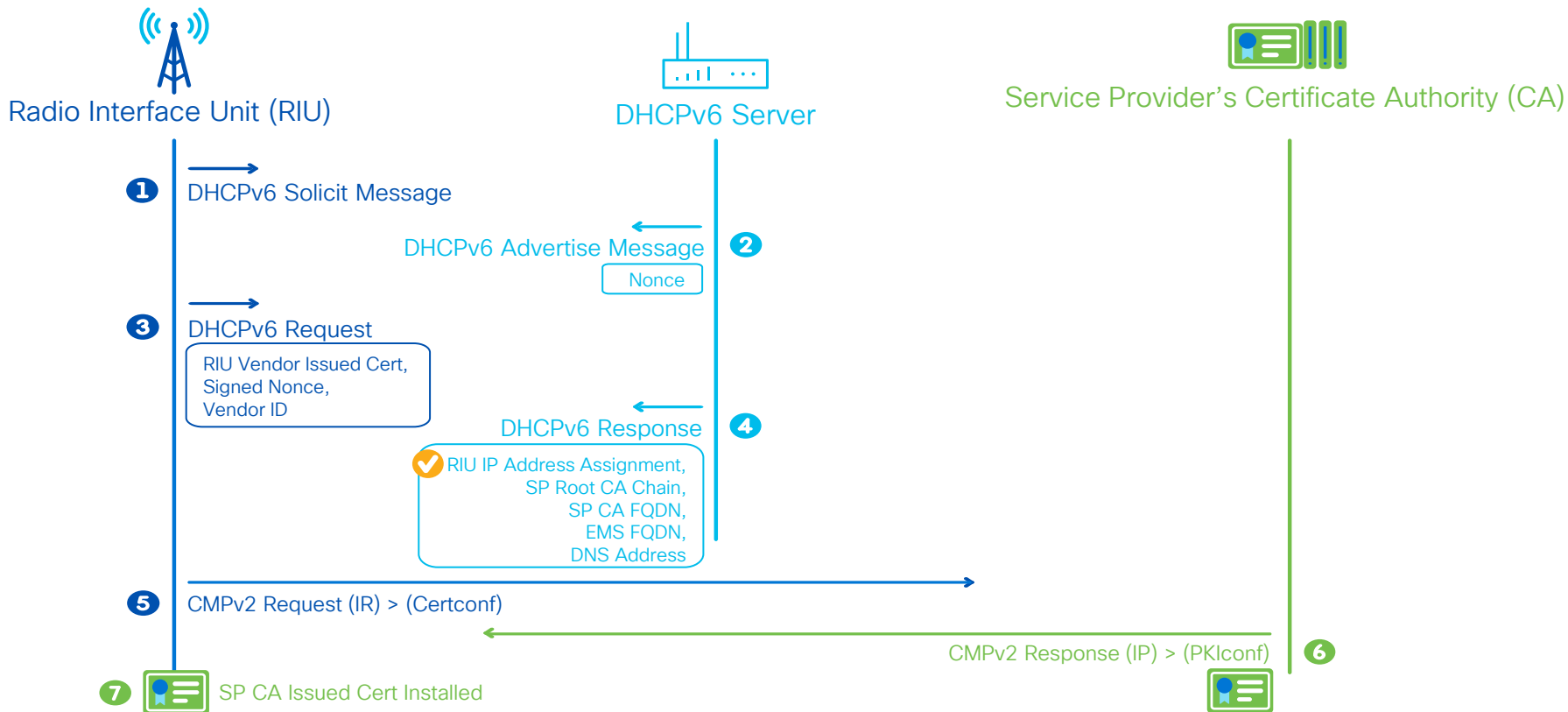
  (DDoS/Malware/DPI/L4FW)

Segmentation

- Which solution to go with?

  (Macro / Micro / Both)*

Visibility

- Which flow data to collect?

  (NetFlow, IPFIX, VPC logs, sFlow, metadata, NSEL, Container Telemetry, Syslog)

Secure RIU Onboarding*

Radio Interface Unit (RIU)

DHCPv6 Server

Service Provider's Certificate Authority (CA)

❶ DHCPv6 Solicit Message

DHCPv6 Advertise Message ❷

Nonce

❸ DHCPv6 Request

RIU Vendor Issued Cert,
Signed Nonce,
Vendor ID

DHCPv6 Response ❹

✅ RIU IP Address Assignment,
SP Root CA Chain,
SP CA FQDN,
EMS FQDN,
DNS Address

❺ CMPv2 Request (IR) > (Certconf)

CMPv2 Response (IP) > (PKIconf) ❻

❼ SP CA Issued Cert Installed

Conclusion

Conclusion

✔ The journey towards 5G needs convergence and an any-G architecture to optimize cost

✔ Hybrid infrastructure now a path to unified NFVI

✔ Special design consideration for Network slice and Right node selection

✔ 5G moving closer to the edge and becoming public

✔ Security needs to be an integral part of 5G with Zero trust, Segmentation, Threat Protection, and Visibility

5G Sessions to attend

Sessions	Description
BRKSPM-1005	MEC Enablers for 5G Networks
BRKSPM-2977	5G Transport Architecture
BRKSPG-2038	Cisco Ultra Cloud Core – Taking 2G, 3G, 4G and 5G towards a common cloud-based mobile core future.
BRKSPM-2027	Holistic Security in 5G deployments

Cisco-Cx

5G Whitepaper – [4G to 5G Migration](#)

Cisco Cx - [https://www.cisco.com/c/m/en_us/customer experience/index.html](#)

Private 5G Whitepaper – [A journey towards Converged 5G Architecture](#)

Technology perspective – [Latest technology trends](#)

UUT Based network slice selection – [Defensive Publication](#)

Technical Session Surveys

- Attendees who fill out a minimum of four session surveys and the overall event survey will get Cisco Live branded socks!

- Attendees will also earn 100 points in the Cisco Live Game for every survey completed.

- These points help you get on the leaderboard and increase your chances of winning daily and grand prizes.

Cisco Learning and Certifications

From technology training and team development to Cisco certifications and learning plans, let us help you empower your business and career. www.cisco.com/go/certs

Pay for Learning with Cisco Learning Credits

(CLCs) are prepaid training vouchers redeemed directly with Cisco.

Learn

Cisco U.
IT learning hub that guides teams and learners toward their goals

Cisco Digital Learning
Subscription-based product, technology, and certification training

Cisco Modeling Labs
Network simulation platform for design, testing, and troubleshooting

Cisco Learning Network
Resource community portal for certifications and learning

Train

Cisco Training Bootcamps
Intensive team & individual automation and technology training programs

Cisco Learning Partner Program
Authorized training partners supporting Cisco technology and career certifications

Cisco Instructor-led and Virtual Instructor-led training
Accelerated curriculum of product, technology, and certification courses

Certify

Cisco Certifications and Specialist Certifications
Award-winning certification program empowers students and IT Professionals to advance their technical careers
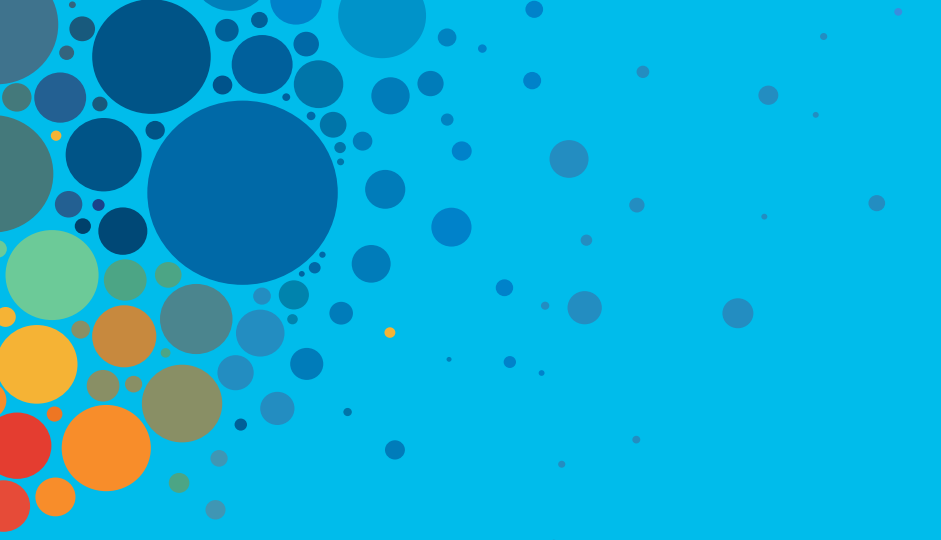
Cisco Guided Study Groups
180-day certification prep program with learning and support

Cisco Continuing Education Program
Recertification training options for Cisco certified individuals

Here at the event? Visit us at The Learning and Certifications lounge at the World of Solutions

Continue your education

- Visit the Cisco Showcase for related demos

- Book your one-on-one Meet the Engineer meeting

- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs

- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

CISCO *Live!*

Thank you

CISCO Live!

ALL IN

#CiscoLive