Next Generation CCIE

Erik Vangrunderbeek (Technical Manager, Learning@Cisco)
Kashif Zeeshan (Exam Program Manager, Learning@Cisco)
BRKCCIE-3352
Questions?
Use Cisco Spark to communicate with the speaker after the session.

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

Cisco Spark spaces will be available until July 3, 2017.

cs.co/ciscolivebot#BRKCCIE-3352
Agenda

• The evolution of CCIE
• Evolving technologies highlights
• How to stay up to date?
• Q&A

“It’s not the strongest of the species that survives, nor the most intelligent, but the one most responsive to change.”

(Charles Darwin)
The Evolution of CCIEs

Changing Priorities: Role, Technologies

Leading…

Strongly involved in today..

Accelerating…

CCIEs are preparing for..

<table>
<thead>
<tr>
<th>Area</th>
<th>% of CCIEs Prioritizing Area</th>
</tr>
</thead>
<tbody>
<tr>
<td>Design/Architecture</td>
<td>58</td>
</tr>
<tr>
<td>Data Center</td>
<td>41</td>
</tr>
<tr>
<td>Network Optimization</td>
<td>36</td>
</tr>
<tr>
<td>SDN</td>
<td>33</td>
</tr>
<tr>
<td>Systems Integration</td>
<td>30</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Area</th>
<th>% of CCIEs Prioritizing Area</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud</td>
<td>35</td>
</tr>
<tr>
<td>Network Programming</td>
<td>28</td>
</tr>
<tr>
<td>Internet of Things</td>
<td>23</td>
</tr>
<tr>
<td>Project/Product Mgmt</td>
<td>20</td>
</tr>
<tr>
<td>Analytics</td>
<td>8</td>
</tr>
</tbody>
</table>

Source: L@C Customer Insights Survey, Cisco, November 2016
The Evolution of CCIEs

Shifting Job Scope and Function for CCIEs

Traditional skills  The Hybrid Engineer  New skills

BRKCCIE-3352 © 2017 Cisco and/or its affiliates. All rights reserved. Cisco Public
Cisco Certifications Evolution

Baseline Skills

- Security
- Cloud
- IoT and Data Analytics
- Business Skills
- Network Programmability

- Architect
- CCIE
- CCNP
- CCNA
- CCENT

Certifications:
- CCNA Industrial (IoT)
- CCNA Cyber Ops
- CCNA/NP Cloud
- Network Programmability Specialist
CCIE Program Updates

Last 1 year

- **CCIE Data Center v2.0**
  - July 2016
  - All written BPs incorporate new Evolving technology domain

- **CCIE SECU v5.0**
  - January 2017
  - Learning Matrix

- **CCIE SP v4.1**
  - June 2017
  - Continuing Education

- **CCIE WIR v3.1**
  - November 2018
  - Agile
## CCIE – Evolving Technologies

### Blueprint Weights

<table>
<thead>
<tr>
<th>WRT%</th>
<th>LAB%</th>
</tr>
</thead>
<tbody>
<tr>
<td>10%</td>
<td>N/A</td>
</tr>
</tbody>
</table>

### Evolving Technologies (Common across all Tracks)

<table>
<thead>
<tr>
<th>REST API</th>
<th>SDN</th>
<th>IoT</th>
<th>DevOps</th>
<th>XaaS</th>
<th>Automation and Orchestration</th>
<th>OpenStack</th>
<th>Cloud</th>
<th>NFV/AFV</th>
</tr>
</thead>
<tbody>
<tr>
<td>CCIE Data Center</td>
<td>CCIE SP</td>
<td>CCIE Security</td>
<td>CCIE Wireless</td>
<td>CCIE Collaboration</td>
<td>CCIE R&amp;S</td>
<td>CCDE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>90%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>100%</td>
<td></td>
</tr>
<tr>
<td>100%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>100%</td>
<td></td>
</tr>
</tbody>
</table>

- **New Evolving Technologies** section added to all CCIE/CCDE tracks, focusing on Cloud, Network Programmability and IoT.
- Future proofing IT professional skills
- **Focus on conceptual understanding** and impact to the current network.
CCIE Learning Matrix

About Study Materials

Use the following resources to supplement your learning experience and exam preparation. This list is comprised of materials suggested by the exam development team to prepare a candidate for the examination.

Learning Matrix

The learning matrix has been developed to allow you to customize your exam preparation. The matrix will provide you with a list of recommended training and resources related to the exam topics.
- CCIE Routing and Switching Learning Matrix
- Evolving Technology Learning Matrix

Suggested Training

Cisco provides a flexible and integrated learning program using instructor-led and self-paced training, hands-on exercises, assessments, and practice exams to build the expert skills required for CCIE certification. The Cisco Expert-Level Training for CCIE Routing and

Learning Matrix: https://learningnetwork.cisco.com/community/learning_center/study_learn_content
Learning Matrix Resources

White papers
Reference books with specific chapters identified
Cisco® Validated Design documents
Cisco Live! 365 presentations
Training courses
Webinars
VoDs
Solution Reference Network Designs (SRNDs)
Case studies, design guides, Design TechNotes, reference guides, etc.

The matrix focusses primarily on Cisco and Cisco Press content
Minor Revisions

<table>
<thead>
<tr>
<th>Definition</th>
<th>Minor Revisions</th>
<th>Major Revisions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency</td>
<td>Minor revision entails smaller but frequent changes to the exam track</td>
<td>Major revision entails larger infrequent changes to the exam track</td>
</tr>
<tr>
<td>Blueprint (Exam Topics)</td>
<td>Every 1-2 years</td>
<td>Every 3-5 years</td>
</tr>
<tr>
<td>Percent Change</td>
<td>Below 20%</td>
<td>Above 20%</td>
</tr>
<tr>
<td>Software Changes</td>
<td>Yes (if needed)</td>
<td>Yes</td>
</tr>
<tr>
<td>Hardware/Equipment Model</td>
<td>Yes, but kept to a minimum (focus on Virtualization, or EOL)</td>
<td>Yes</td>
</tr>
<tr>
<td>Changes (including real &amp;</td>
<td>~ 4 months</td>
<td>~ 6 months</td>
</tr>
<tr>
<td>virtual), and EOL devices</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Notification / Announcement</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Sample: Major Minor Minor Minor Major ?

https://learningnetwork.cisco.com/community/expert-level-certifications-agile-blueprints
Continuing Education Program

- A flexible alternative **option** to recertify
- To encourage candidates to diversify their skill sets
- Currently ONLY available for CCIE candidates only (in active or suspended state)
- Starts June 6th

---

<table>
<thead>
<tr>
<th>Option 1 : Written exam</th>
<th>Option 2: Continuing Education</th>
</tr>
</thead>
<tbody>
<tr>
<td>Take the qualification exam (no policy change)</td>
<td>1. Enroll to the program</td>
</tr>
<tr>
<td></td>
<td>2. Earn 100 credits (by completing any of the approved offerings)</td>
</tr>
<tr>
<td></td>
<td>3. Administrative fee</td>
</tr>
</tbody>
</table>

https://ce.cisco.com/
Continuing Education Program
Dashboard

Samples:
CCIE Techtorial (8hrs)  10
Item authoring  21
Cisco Digital Network Architecture Implementation Essentials  40
Developing with Cisco Network Programmability  50
Continuing Education Program

Business Rules

- Credits, once earned, will be valid for three years from the date they were earned.
  - Credits will expire if a new recertification cycle starts, i.e., by passing an exam.
  - Credits will expire if your certification becomes inactive before completing the CE requirements.

- Credits earned for a given course can only be counted once within the recertification cycle.
- Repeating the same course will not count towards recertification credits.
- Credits, once used, cannot be reused for any other certification track or level.
- Credits must be used (1) before they expire, or (2) during the certification cycle in which they were earned, whichever occurs earlier.

- The Continuing Education administrative fee will need to be paid once you have earned the required number of credits. You can pay the fee by visiting https://ce.cisco.com.

https://learningnetwork.cisco.com/community/certifications/cisco-continuing-education-program
3D/Virtual Reality
Developed by the CCIE team

- Industry first from industry leader
- State-of-the-art Virtual Reality (VR) solution
- 3D visualization of technical content
- Interacts with simulated physical environment and virtualized infrastructure
- Custom API that integrates IOL with VR application
Virtual Reality

BeTheRouter (BTR)

TroubleshootTheLab (TTL)

Available in the Certifications Lounge
June 26-29

Live DEMO in the Certification Lounge!
What is next?

- Continuing Education
- Quality
- Recertification
- Integrity
- Study Material
- Evolving Technologies
- Virtual Reality
- Relevancy
Evolving technologies highlights (Cloud, OpenStack, Network Programmability, IoT)
Cloud
Compare and contrast Cloud deployment models
Evolving Technologies Blueprint for Cloud Domain

https://learningnetwork.cisco.com/community/ccie-enhancements

<table>
<thead>
<tr>
<th>Compare and contrast Cloud deployment models</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Infrastructure, platform, and software services (XaaS)</td>
</tr>
<tr>
<td>• Performance and reliability</td>
</tr>
<tr>
<td>• Security and privacy</td>
</tr>
<tr>
<td>• Scalability and interoperability</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Describe Cloud implementations and operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Automation and orchestration</td>
</tr>
<tr>
<td>• Workload mobility</td>
</tr>
<tr>
<td>• Troubleshooting and management</td>
</tr>
<tr>
<td>• OpenStack components</td>
</tr>
</tbody>
</table>
Cloud Computing Defined

National Institute of Standards and Technology Cloud Model

Essential Characteristics
- Measured Service
- Rapid Elasticity
- On-Demand Self Service
- Broad Network Access
- Resource Pooling

Service Models
- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)

Deployment Models
- Public
- Private
- Hybrid
- Community
Cloud Service Models

On-Prem

- Application
- Data
- Runtime
- Framework
- Middleware
- Services
- OS
- Virtualization
- Servers
- Storage
- Networking

Managed by Provider

Undifferentiated Heavy Lifting

IaaS

- Application
- Data
- Runtime
- Framework
- Middleware
- Services
- OS
- Virtualization
- Servers
- Storage
- Networking

Managed by Provider

PaaS

- Application
- Data
- Runtime
- Framework
- Middleware
- Services
- OS
- Virtualization
- Servers
- Storage
- Networking

Managed by Provider

SaaS

- Application
- Data
- Runtime
- Framework
- Middleware
- Services
- OS
- Virtualization
- Servers
- Storage
- Networking

Managed by Organization
It’s a hybrid IT world

81% Evaluating or using public cloud
73% Have a hybrid cloud strategy
84% Will use multiple clouds

SECURITY  LATENCY  PRIVACY

Thing > Network > Cloud > Analytics > Apps

SCALABILITY  RELIABILITY
Infrastructure and Application Evolution

Traditional Applications
ERP, CRM, Financial, Client/Server, email, …

Cloud Native Applications
IoT, Big Data, Analytics, Gaming, ...

Data Center
Cloud
Edge / IoT
But It’s Not Easy

A Tale of Two Operating Models

Cloud Native

Traditional
Cloud Application Maturity Spectrum

Application architectures leverage capabilities “Native” to cloud infrastructure that benefit security, performance, operations and service management.

<table>
<thead>
<tr>
<th>Service Oriented</th>
<th>Legacy</th>
<th>Tolerant</th>
<th>Ready</th>
<th>Native</th>
</tr>
</thead>
<tbody>
<tr>
<td>Self-Describing</td>
<td>Provided Externally</td>
<td>Provided Externally</td>
<td>Minimum Contract; Default Policy Only</td>
<td>Complete Contract and Policy</td>
</tr>
<tr>
<td>Publish/Subscribe</td>
<td>Manually at Design</td>
<td>Manually at Design</td>
<td>Publish Automatic; Subscribe Manual</td>
<td>Publish &amp; Subscribe (Automatically)</td>
</tr>
<tr>
<td>Portability/Mobility</td>
<td>Varies (No/Minimal Packaging; Fixed Location)</td>
<td>Varies (Minimal Packaging; Limited Location Change)</td>
<td>Complete Packaging; Regional Location Change</td>
<td>Complete Packaging; Global Movement</td>
</tr>
<tr>
<td>Fault-Tolerant</td>
<td>None; Manual Intervention</td>
<td>None; Manual Intervention</td>
<td>Completely Automated</td>
<td>Completely Automated</td>
</tr>
<tr>
<td>Elastic</td>
<td>None; Manual Provision</td>
<td>Grow; Dynamic Provision</td>
<td>Grow &amp; Shrink; Dynamic Provision</td>
<td>Optimized; Dynamic Discover &amp; Provision</td>
</tr>
<tr>
<td>Stateless</td>
<td>Varies (Stateful – No State)</td>
<td>No State – Simple External Cache</td>
<td>No State – All State managed externally</td>
<td>No State – All State managed externally</td>
</tr>
<tr>
<td>Self-Defending</td>
<td>Manually at Design (if any)</td>
<td>Manually at Design (if any)</td>
<td>Authentication &amp; Protocols</td>
<td>AAA; Communication; Data (Complete)</td>
</tr>
<tr>
<td>Manageable</td>
<td>Manually at Design</td>
<td>Minimal (Heartbeat; logging)</td>
<td>Adequate (Health; Configurable)</td>
<td>Fully</td>
</tr>
</tbody>
</table>

Application architectures leverage capabilities “Native” to cloud infrastructure that benefit security, performance, operations and service management.
Profile of a Cloud Optimized Organization

<table>
<thead>
<tr>
<th>Category</th>
<th>Percentage</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multicloud Adoption</td>
<td>84%</td>
<td>Expect to choose from multiple cloud providers</td>
</tr>
<tr>
<td>Containers</td>
<td>66%</td>
<td>Believe Containers are important to their Cloud Strategy</td>
</tr>
<tr>
<td>Microservices</td>
<td>79%</td>
<td>Develop application using Microservices</td>
</tr>
<tr>
<td>DevOps</td>
<td>80%</td>
<td>Use DevOps practices</td>
</tr>
<tr>
<td>Governance</td>
<td>82%</td>
<td>Have robust cloud governance policies in place</td>
</tr>
<tr>
<td>Cloud IoT Apps</td>
<td>62%</td>
<td>Have adopted cloud based IoT applications and of those 53% in a private cloud environment</td>
</tr>
<tr>
<td>Cloud Security Apps</td>
<td>40%</td>
<td>Use cloud delivered management of security devices, located on or off-premises</td>
</tr>
</tbody>
</table>
Cloud Neutral approach

A cloud neutral approach to your hybrid IT world
Cloud Security Landscape

- Devices / Users: Anywhere / Anything
- Network: Software Defined Networking
- Application: Microservices Architecture
- Compute: Containers
- Storage: Data Virtualization
## The Changing Cloud Security Threats
### The Treacherous Twelve

<table>
<thead>
<tr>
<th>Year</th>
<th>2010</th>
<th>2013</th>
<th>2016</th>
<th>Top Threats</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>Data Breaches</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>Insufficient Identity, Credentials and Access Management</td>
</tr>
<tr>
<td>6</td>
<td>3</td>
<td>6</td>
<td>6</td>
<td>Insecure Interfaces and APIs</td>
</tr>
<tr>
<td>3</td>
<td>6</td>
<td>7</td>
<td>7</td>
<td>System Vulnerabilities</td>
</tr>
<tr>
<td>5</td>
<td>2</td>
<td>8</td>
<td>8</td>
<td>Account Hijacking</td>
</tr>
<tr>
<td>7</td>
<td>8</td>
<td>9</td>
<td>9</td>
<td>Malicious Insiders</td>
</tr>
<tr>
<td>1</td>
<td>7</td>
<td>10</td>
<td>10</td>
<td>Advanced Persistent Threats</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>11</td>
<td>11</td>
<td>Data Loss</td>
</tr>
<tr>
<td>4</td>
<td>9</td>
<td>12</td>
<td>12</td>
<td>Insufficient Due Diligence</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Abuse and Nefarious Use of Cloud Services</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Denial of Service</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Shared Technology Issues</td>
</tr>
</tbody>
</table>

What is Cloud Security?

- **Who**
- **Risk & Responsibilities**
  - Control Points
  - Trust Boundaries
- **Visibility**
- **Enforcement**
- **Data Protection**

**Data Center**

**Cloud**

- Public
- Private
- Hybrid

**Users/Devices**

**Security Everywhere**
Shared Risk and Responsibility
Cloud Delivery Models

Private Cloud
- Application
- Data
- Guest OS
- Virtualization
- Network
- Facility

IaaS
- Application
- Data
- Guest OS
- Virtualization
- Network
- Facility

PaaS
- Application
- Data
- Guest OS
- Virtualization
- Network
- Facility

SaaS
- Application
- Data
- Guest OS
- Virtualization
- Network
- Facility

Shared Responsibility

Tenant

Provider
New Control Points, Data Protection

Users / Devices

DAM (Data-At-Motion)

Visible pipe
Weak encryption
Key compromise

Rogue/Weak/Dirty Applications

Data visibility
Data loss

Stolen Credentials
Malware
Spoofing
Pivot

Compute

Data-At-Rest (DAR)

Cisco live!
Securing the Connectivity to Cloud Platform

- **Customer Network (MPLS/VPN)**
- **Internet**
- **Remote Site**
- **Data Center**
- **Cisco Routers ASA / NGFW**
- **Service Provider**
- **Verizon SCI**
- **AT&T NetBond**
- **Level3 Cloud Connect**
- **IXP X-Connect Partner**
- **Direct Connect**
- **Cloud**
  - Tenant space
  - PaaS
  - SaaS

**Encryption**
- Virtual Connectivity
  - ICF, VPN, Application SSL
Cloud Edge Model

Rebuilding the perimeter with next generation, multi-service, cloud platform…

BIG DATA ANALYTICS: CROSS CUSTOMER & CROSS PRODUCT

- DNS-BASED ATD
- SECURE WEB GATEWAY
- STANDALONE SANDBOX
- CASB
- THIRD PARTY INTEGRATIONS

MULTI TENANCY, CENTRALIZED ADMINISTRATION, SCALABLE REPORTING

CLOUD PLATFORM
Cloud Requires Trust
Cloud Requires Trust

Visibility
Sharing Info
Documentation

$3^{rd}$ Party
Validation &
Certification

Process

Security and
organizational
controls
Cloud and Security Standards

Keywords:
- HIPPA
- COBIT
- ISO 27001
- ISO 15000
- ISO 20000
- NIST
- CISP
- ITIL
- PCAOB
- BS
- EVSSL
- SAS
- SysTrust
- CMM
- PCI-DCC
- QL 827
- SOX 404
- WebTrust
Cloud Security Standards Work

- CSA
- DMTF
- CloudAudit
- NIST
- ISO
- ITU-T
- IEEE
- IETF
- SNIA
- TMF
- OASIS
- OCC
- MEF
- OCC
- OCM
- ISOC
- NCOIC
- CCIF
- OGF
CSA STAR is based upon two key research components of the CSA GRC Stack:

- **Cloud Controls Matrix (CCM)** - As a controls framework, the CSA CCM provides organizations with the needed structure, detail and clarity relating to information security tailored to cloud computing. Currently 133 Controls.

- **The Consensus Assessments Initiative Questionnaire (CAIQ)** - Based upon the CCM, the CAIQ provides a set of Yes/No questions a cloud consumer and cloud auditor may wish to ask of a cloud provider to ascertain their compliance to the Cloud Controls Matrix and CSA best practices.
Industry Regulatory Compliance Guidance

• **PCI DSS - Credit Card Data and Processors Protection.** Assess hosting company environments that are dealing with multi-tenant issues

• **FedRAMP – FISMA-NIST-800-53** - Government Agencies and their Service Providers. Assist clients in assessing and meeting FISMA requirements to attract Government agency business moving to the cloud as part of FedRAMP

• **HIPAA/HITECH – Health Care** Segment. Bringing multi-location medical centers and healthcare organizations into compliance

• **ISO 27001 (2013)** - Provides requirements for establishing, implementing, maintaining and continuously improving an Information Security Management System (ISMS) "Bringing multi-location medical centers and healthcare organizations into compliance

• **ISO 27018 (2014)** - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

• **ISO 27017 (2015)** - Code of practice for information security controls based on ISO/IEC 27002 for cloud services

• **SOC1 / SOC2** - SOC 1 is the reporting option for which the SSAE 16 professional standard is used, resulting in a **SOC 1 SSAE 16 Type 1** and/or a **SOC 1 SSAE 16 Type 2** report. SOC 2 is the reporting option which was specifically designed for many of today's cloud computing, Software as a Service (SaaS), and technology related service organizations.
Cloud Implementations and Operations
Workload provisioning profile & policy

Provisioning Drivers
- Risk, Compliance, Business Impact
- Performance & Dependencies – *Tier options*
- Cost – *Tier options*
- Data & Distribution
- Infrastructure & Application requirements

Cloud Patterns
- Host/Cluster affinity/anti-affinity
- Load balancing / Application Proxy

http://cloudpatterns.org/compound_patterns/resource_workload_management
Define policies for Cloud Workload Placement

Develop a strategy that incorporates all policy and performance requirements that leverages automation and orchestration.

1,000’s of unique instances are managed independently on the same platform.

- **Service A**: IO intense, low risk workload
- **Service B**: Memory intense, PCI data sensitive workload
- **Service C**: CPU Intensive, locale sensitive workload

Microsegment:
- VLAN100
- VLAN200
- VLAN300

security & performance zones
Cloud Management Solutions

Industry experts agree, a new cloud management platform is needed:

- Single management platform
- Application-centric
- Workloads are portable
Cloud Management Platform Services

- Single Integrated Management Platform
- Full Application Lifecycle Management
- Enterprise-Ready
- Scalable
- Secure
What is Openstack?

• To produce the ubiquitous **Open Source Cloud Computing platform** that will meet the needs of **public and private clouds** regardless of size, by being **simple to implement and massively scalable.**
Core OpenStack Projects / Components

**Compute**
- "Nova"
  - Controls Virtual Machines
  - Support for multiple hypervisors

**Storage**
- "Glance, Swift, Cinder"
  - Image, Object, Block
  - Instance/VM image storage
  - Cloud object storage
  - Persistent block storage

**Dashboard**
- "Horizon"
  - Web app for controlling OpenStack resources
  - Self-service portal
  - Only uses APIs to access services

**Identity**
- "Keystone"
  - Centralized Policies
  - Tenant Management
  - RBAC
  - External integration (LDAP)

**Networking**
- "Neutron"
  - Networking service
  - IP address mgmt
  - Public / Private Networks - NAT
  - Plugins to external HW
  - LBaaS / FWaaS

**Metering**
- "Ceilometer"
  - Metering and monitoring
  - Central collection point

**Orchestration**
- "Heat"
  - Template-based orchestration engine
  - Faster deployment of applications

**Bare-Metal Provisioning**
- "Ironic"
  - Bare-Metal Provisioning
  - Use of PXE/IPMI

**Containers**
- "Magnum"
  - Capability to offer containers to cloud users

**Containers**
- "Kolla"
  - Containerization of OpenStack Services

[https://www.openstack.org/software/project-navigator/](https://www.openstack.org/software/project-navigator/)
Sample questions

Infrastructure, platform, and software services (XaaS)

Which option describes the characteristics of a public Infrastructure as a Service cloud service model?

A. It is a way of delivering cloud-computing infrastructure (servers, storage, network, and operating systems) as an on-demand service.

B. It is a cloud-computing platform that facilitates the creation of web applications without the need to maintain the supporting software applications.

C. It is a cloud service where the underlying hardware is managed by the cloud service provider.

D. It is a cloud-computing platform that facilitates the creation of web applications without the need to maintain the supporting software operating systems.
Learning Matrix for Cloud Domain

Cisco Press Books – Suggested Reading

- Designing Networks and Services for the Cloud (ISBN-10: 1-58714-294-5)

Cisco Courses

- Automating the Cisco Enterprise Cloud (CLDAUT)
- Implementing and Troubleshooting the Cisco Cloud Infrastructure (CLDINF)
- Designing the Cisco Cloud (CLDDES)

Cisco Live Presentations

- BRKCLD-2008 - Multi-Cloud and Application Centric Modeling, Deployment and Management with Cisco CloudCenter
- LABCLD-2330 - Hybrid Cloud. Migrate your Application from Private ACI cloud to Public AWS Cloud
- BRKCLD-2000 - Cloud Types and Security - What they Mean to You and Your Company
- BRKSEC-2404 - Effective Cloud Security Made Simple – Cloud Security Re-imagined with CloudLock

Other References

Network Programmability
Describe functional elements of network programmability and how they interact
## Evolving Technologies Blueprint for Network Programmability

Describe functional elements of network programmability and how they interact

- Controllers
- APIs
- Scripting
- Agents
- Northbound vs. Southbound protocols

Describe aspects of virtualization and automation in network environments

- DevOps methodologies, tools and workflows
- Network/application function virtualization (NFV, AFV)
- Service function chaining
Ingredients of Hybrid IT

- **Application Centricity**
- **Programmability** of
  - Infrastructure
  - Controllers
  - Services
- **Virtualization** of
  - vAF: Application Functions
  - vMF: Management Functions
  - vNF: Network Functions

---

Bimodal IT Architectures to support Fast IT Business Needs
Pace of change and Networks

Network Expenses

- CAPEX: 33%
- OPEX: 67%

Deployment Speed

- Computing: 0 seconds
- Networking: 1000 seconds

Source: Forrester

- 80% Time IT spends on operations
- 55% CMOs think IT is not responding fast enough to time-sensitive projects
- 57% CEOs are worried about IT strategy not supporting business growth

Source: Open Compute Project
Evolving Our Interaction with Network OS

Types of Interactions
- Bootstrap
- Configure
- Monitoring
- Extend

What's Evolving
- Manual → Automated
- Static → Dynamic
- Generic → Custom

Why?
- Agility
- Scale
- Cost
- Complexity
How > 70% of Config Management is Done Today

zaphod# conf t
Enter configuration commands, one per line. End with CNTL/Z.
zaphod(config)#

“It's the way real men build real networks.”

- Task Oriented
- Human Friendly
- Easy To Replay
- No Special Tools
- Software Unfriendly
- Subject To Change
- No Common Data Model
- No Error Reporting
Ways to Automate Network Components

On Box:
```
#!/usr/bin/env python
print('Hello World!')
```

Off Box:
```
#!/usr/bin/env python
print('Hello World!')
```

via SDN Controller:
```
#!/usr/bin/env python
print('Hello World!')
```
Programmability – SDN

Northbound Programmability Layer

SDN Control Plane

Southbound Programmability Layer

OpFlex, Netconf, YANG, CLI, NX-API, BGP-EVPN, Openflow

Virtualized Environment

OVS, VTF, AVS

Switch, Nexus 9K, Routers

Automation, Hypervisor Management, Enterprise Monitoring, Systems Management, Orchestration Frameworks, Applications

REST API, SDK, Plugins

VTS, APIC, APIC-EM, ODL
Options for Programming the DC Network

Programmable Network
Traditional 2/3-Tier

Programmable Fabric
Open Controller Model

Integrated Fabric
Cisco APIC

- Modernized Operating System
- Programmable Open APIs
- HW & SW Disaggregation

- L2 / L3 Overlay & Underlay
- Physical & Virtual End points
- Decoupled Controllers
- VXLAN Overlay

- Any Hypervisor
- Physical. Virtual / Open API's
- Day 1 & 2 Ops
- Gartner: ACI outpacing competitors by 2x to 5x
Requirements of Next-Gen Config Management

- Easy to Use
- Separates Config and Operational Data
- Configuration of Network as a whole
- Common database schema
- Error Checking
- Backup/Restore Capability
- Human & Machine Friendly

RFC 3535
CY 2002
Result: NETCONF and YANG

**NETCONF**
- IETF standard – RFC 6241
- Designed for network programmability
- Session and connection oriented
- Runs over SSH or SOAP

**YANG**
- IETF standard – RFC 6020, 6021
- Data Modeling language for networking (config & state)
- Explicitly & precisely defines the structure, syntax & semantics of data
- Represents data structures in XML tree format

**RESTCONF**
- IETF draft
- Designed for web applications (REST “like”, based on NETCONF)
- Access data defined in YANG using datastores defined in NETCONF
- Runs over HTTP/S
Netconf

NETCONF (Network Configuration Protocol)
- IETF protocol for configuration data and operational state data management & notifications
- Addresses SNMP SMI short-comings like no transactions, no backup&restore, strange&legacy concepts…
- Based on XML (Yang to provide the data modeling)
- 830/tcp – runs over SSH (possibly also TLS, BEEP…)

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="101"
     xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
    <get-config>
        <source>
            <running/>
        </source>
        <filter
            xmlns:if="urn:ietf:params:xml:ns:yang:ietf-interfaces"
            type="xpath"
            select="/if:interfaces/if:interface[if:name='eth0']"/>
    </get-config>
</rpc>
```
## Netconf and Restconf

RPC (Remote Procedure Call) operations to access config and state data

1. **NETCONF** *(RFC6241)* – for networking community (feels like a Protocol)
   - **XML** format, defined operations
   - Runs over SSH/TLS/...

2. **RESTCONF** *(draft-bierman-netconf-restconf)* – for developers community (feels like an API)
   - **JSON** or **XML** format, uses standard HTTP and its methods: **GET, POST, HEAD**...
   - **ReST** (Representational State Transfer) based – a software architectural style used in Web services

<table>
<thead>
<tr>
<th>NETCONF (XML)</th>
<th>RESTCONF (HTTP)</th>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;get&gt;</td>
<td>HTTP GET</td>
<td>Get operational data (like “show” commands)</td>
</tr>
<tr>
<td>&lt;get-config&gt;</td>
<td>HTTP GET</td>
<td>Get configuration (like “show run”)</td>
</tr>
<tr>
<td>&lt;edit-config&gt;</td>
<td>HTTP PATCH</td>
<td>Edit configuration (like “conf t” and then “commit”)</td>
</tr>
<tr>
<td>&lt;edit-config&gt; operation=“delete”</td>
<td>HTTP DELETE</td>
<td>Delete configuration (eg. like “no int lol11”)</td>
</tr>
<tr>
<td>&lt;edit-config&gt; operation=“create”</td>
<td>HTTP POST</td>
<td>Create configuration (eg. like “int tunnel-te 100 ...”)</td>
</tr>
<tr>
<td>&lt;edit-config&gt; operation=“replace”</td>
<td>HTTP PUT</td>
<td>Replace configuration</td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
YANG

YANG (RFC6020 etc.) is a data modelling language

- “Yet Another Next Generation” – developed after the NG-SNMP fiasco
- Data modelling for NETCONF protocol, and more: XML conversion, visualization, code generation...
- NETCONF/YANG’s ambition is to provide the ultimate multi-vendor R/W element and service management, thus an open standard programmability architecture

For example, I can use YANG to describe:

- a data structure of a routing protocol
- RIB, FIB, ARP table, MAC table...
- Anything we use „show command“ or MIB for

Or also:

- a communication protocol (header fields, options...)
- Auto-generate code (eg. Java) for it

And also a Service:

- MEF E-Line – UNI attributes
- IP VPN service – contract, SLA, QoS...

YANG vs. SNMP

<table>
<thead>
<tr>
<th></th>
<th>YANG</th>
<th>SNMP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Framework (definition language)</td>
<td>YANG</td>
<td>SMI</td>
</tr>
<tr>
<td>Content (information model)</td>
<td>YANG module</td>
<td>MIB</td>
</tr>
<tr>
<td>Payload (encoded data)</td>
<td>XML (ASCII)</td>
<td>ASN.1 BER (binary)</td>
</tr>
<tr>
<td>Protocol (remote access)</td>
<td>NETCONF, RESTCONF</td>
<td>SNMP</td>
</tr>
</tbody>
</table>
Programmability – Off-box

Data Model

Configuration
- Standard
- Device Specific

Operational
- Standard
- Device Specific

Device Features
- Interface
- BGP
- QoS
- ACL
- ...

Web App
Netconf Client
RestConf
NetConf
The Full Stack – IT picture

- **APIs** so that the **network** infrastructure can be **programmed**

- Program the network infrastructure to support **automation**

- To make **automation** work across the organization, you need **DevOps**
“I can spin up servers in minutes with my Configuration Management Tool workflows, why does it take orders of magnitude more to spin up and affect change on my Network Elements?”

1 IT engr to 10 physical servers — Gartner

1 IT engr to 30,000 virtual servers — Facebook 2013
DevOps: Applying IT Automation Tools to Networks

Intent-based
Master/client
Agent-driven (mostly)
DevOps: Automation Tools

Agent

- "Pull based" with agent
- Agent on managed device connects with master for config information periodically
- Changes made on master are pulled down and executed
- Operations are Idempotent

Agent-less

- Agent-less CM are "pushed based"
- CM scripts are run on the master
- Scripts connect to the managed device and execute the tasks
- No timer, control lies with the master
- Operations are Idempotent
Automating Device Operational Lifecycle

GOAL: Get a device/s into an operational state?

CHALLENGE: “I can bring up a server in 5 minutes, but a switch takes 2 days…”

GOAL: Get the network into an operational state?

CHALLENGE: Automation of configuration for servers and applications is relatively easy how can my network be as easy?

GOAL: Continuously upgrade features within my network, incrementally and safely?

CHALLENGE: I can dynamically patch Linux with automated tools why can’t I do the same with my network devices?

GOAL: Add dynamic services, optimize behavior and troubleshooting?

(Includes information from applications and the network correlated)

CHALLENGE: My compute and application platforms are open and extensible why is my network not?

Ignite & POAP/PXE

Ansible, Puppet and Chef

NX-API/REST

Ansible

Puppet and Chef

Guestshell

Modular NX-OS

Patchablity

ISSU

Guestshell

Splunk/Nagios

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Public
Puppet & Chef on Cisco Nexus

Native NX-OS

- NXOS VSH (CLI)
- NXOS Services
- NXOS Root FS (WRL5)
- Kernel (WRL5)
- Customer Intent
- Cisco Resource & Provider
- Cisco Utilities
- Cisco WRL5 Puppet Agent/Chef Client

Supported on Cisco Nexus 3000 and Nexus 9000 series platforms

Container Based

- NXOS VSH (CLI)
- NXOS Services
- NXOS Root FS (WRL5)
- Kernel (WRL5)
- LXC
- Customer Intent
- Cisco Resource & Provider
- Cisco Utilities
- Cisco CentOS Puppet Agent/Chef Client

Supported on Cisco Nexus 3000, Nexus 5000, Nexus 7000 and Nexus 9000 series platforms
Summary – the Network Isn’t Isolated Anymore
Network Programmability
Describe aspects of virtualization and automation in network environments
What is NFV?

Classical Network Appliance Approach

- Fragmented, purpose-built hardware
- Physical install per appliance per site
- Hardware development large barrier to entry for new vendors, constraining innovation & competition

Network Functions Virtualisation Approach

Orchestrated, automatic & remote install

High volume standard servers, storage, Ethernet

Move Network Function to SW

What is NFV?

Classical Network Appliance Approach

- Message Router
- CDN
- Session Border Controller
- WAN Acceleration
- DPI
- Firewall
- Carrier Grade NAT
- Tester/QoE monitor
- SGSN/GGS N
- PE Router
- BRAS
- Radio/Fixed Access Network Nodes

Network Functions Virtualisation Approach

- vRR
- vPE
- DHCP

Modular

High volume standard servers, storage, Ethernet

Orchestrated, automatic & remote install

Move Network Function to SW
Buzz words associated with NFV

- Hypervisor
- OpenStack
- VIM
- OPNFV
- VNF
- Open Virtual Switch
- vCPE
- KVM
- SDN
- Intel-DPDK
- SR-IOV
- OpenDayLight
- VPP
- NSH
ETSI NFV Reference Architecture

NFV-O
Cisco NSO
(Orchestrator)

VNF-M
(app-specific)
- Cisco ESC (wireline)
- Cisco TCM (mobile)
- Generic (HEAT)

VIM
Virtualized
- OpenStack, vCenter
- Cisco vBN (scale)
- Optional SDN-Ctrl

Services Lifecycle
- Realize services
- Cross-domain

VNF Lifecycle
- Monitoring
- Elasticity (Scale)
- Fault Recovery
- Initial Config

Resource Mgmt
- Multi-Hypervisor
- pCPU → vCPU
- VM or LXC
- Boot mgmt
- HA...

NFV Management and Orchestration (MANO)

BSS

OSS

EMS1
EMS (app-specific)
Cisco NSO (NED), PRIME

EMS2

EMS3

VNF
VNF (app-specific)
Cisco CSR1Kv, XR9Kv, vASA, vIPS, vE/WSA,…

VNF1

VNF2

VNF3

NFVI (Infrastructure)

Virtual

Virtual

Compute/Storage

Cisco UCS, Controller/Director

Computes

Commercial (ESXi, Hyper-V, XEN)

SDN subsys

vSwitch: VTF, OVS, AVS

SDN-C: VTS, ODL, APIC

VIM

VIM virtualized

VnF

Nf-Nf

Nf-Vi

Ve-Vnfm

Vi-Vnfm

OpenPnP

PnP Server

NED

CLI, SNMP

PNF

PNF

direct Netconf/Yang

Physical Backbone, R1/R2 (eg. Cisco ASR)

Defined by OPNFV
https://www.opnfv.org/
OpenDaylight SDN Controller

Key Highlights
- Linux Foundation – true open source project (no company controls this)
- Yang based (MD-SAL)
- Simple to install & use (java)

Cisco OSC (Open SDN Controller)
- Commercial distribution of ODL
- Removed some sub-projects
- Added:
  - Cisco TAC and Devnet support
  - HA Clustering, GUI, monitoring, OVA install,…”
- Support:
  - Openflow and OVSDB (Nexus, ASR9K, OVS)
  - Netconf/Yang (ASR9K, VTF…)
  - BGP-LS, PCEP (ASR9K…)
Open SDN Controller: Carrier Class

Pre-Installed Apps

• **BGPLS Manager** - visualizes network topology from BGP database

• **Inventory** – augmented OpenDaylight “Nodes” app identifies all connected devices

• **(YANG) Model Explorer** – exposes system models and previews JSON API body

• **OpenFlow Manager** – manages, visualizes and troubleshoots flows + previews JSON API body

• **PCEP Manager** – creates, modifies and deletes MPLS LSPs

Centralized OA&M

• Robust user, application and feature administration

• Status monitoring; system, cluster, node

• Event logging

• Real-time CPU, memory, disk, heap size, load and network utilization metrics

“One-Click” install

• VMware ESXi and Oracle Virtual Box hypervisor ready
SPs are Approaching NFV in Multiple Ways
Different Solutions Required to Address Different “Buying Centers”

- **Key trend**
  - **Infrastructure Led**
    - Bottom-up approach
    - Buying Center – Network & DC infrastructure team
  - **Use Case Led**
    - Top-down approach
    - Business outcome driven
    - Buying Center – BU/Biz Vertical
  - **Orchestration Led**
    - Common MANO solution for different use cases
    - Buying Center – NMS/OSS team

- **We are leading with vMS & Mobility**

- **SP’s OSS/ESC**
  - Use Case Specific, e.g. vMS, VPC
  - Includes VNF-M and NFV Orchestration
  - Hardware, VIM (OpenStack) and SDN Controller

- **Modular offer with NSO & ESC**

---

BRKCCIE-3352 © 2017 Cisco and/or its affiliates. All rights reserved. Cisco Public
Service Chaining

- Linkage of service functions to realize a service is called **Service Chaining**

- A (logical) classification function selects traffic that needs to be chained
  - The policy can be as simple as match on VLAN or VRF or match flow rules
  - Or it could be complex policies including subscriber ID and application parameters
New Technology Trends
Changing Network Service Insertion Landscape

- In addition to existing complexities of service deployment, networks are evolving, with physical and virtual workloads and services
  - Existing network service insertion techniques cannot remain static and must evolve
  - SDN & NFV enabling control / data plane independence and virtualization of network elements

<table>
<thead>
<tr>
<th>From:</th>
<th>To:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical appliances</td>
<td>Virtual &amp; physical appliances</td>
</tr>
<tr>
<td>Static services</td>
<td>Dynamic services</td>
</tr>
<tr>
<td>Separate domains: physical vs. virtual</td>
<td>Seamless physical &amp; virtual interoperability</td>
</tr>
<tr>
<td>Hop-by-hop service deployment</td>
<td>Chain of “service functions”</td>
</tr>
<tr>
<td>Underlay networks</td>
<td>Dynamic overlay networks</td>
</tr>
<tr>
<td>Topological dependent service insertion</td>
<td>Insertion based on resources &amp; scheduling</td>
</tr>
<tr>
<td>No shared context</td>
<td>Rich metadata</td>
</tr>
<tr>
<td>Policy based on VLANs</td>
<td>Policy based on metadata</td>
</tr>
</tbody>
</table>
Network Service Header (NSH) Architecture
High-level Component Structure

- **Architecture components**
  - Service Chaining Orchestration
    - Define service chains & build service paths
  - Control / Policy Planes
    - Instantiate service chains adhering to policy
  - Data Plane
    - Traffic steering & metadata

![Diagram of NSH Architecture](image)
Sample questions
Automation and orchestration

Considering the ITIL v3 model, what are Puppet and Chef primarily used for?

A. problem management
B. release management
C. configuration management
D. change management
Learning Matrix for SDN Domain

Cisco Press Books – Suggested Reading
- Programming and Automating Cisco Networks

Cisco Courses
- Designing and Implementing Cisco Network Programmability (NPDESI)
- Programming for Network Engineers (MPODF20)

Cisco Recorded Seminars
- https://learningnetwork.cisco.com/community/learning_center/sdn_recorded_seminars

Other References
- SDN Study Guides - https://learningnetwork.cisco.com/docs/DOC-31004
- DevNet Sandbox - https://developer.cisco.com/site/devnet/home/index.gsp
Internet of Things
Describe architectural framework and deployment considerations for IoT
Evolving Technologies Blueprint for IoT

Describe architectural framework and deployment considerations for IoT

• Performance, reliability and scalability
• Mobility
• Security and privacy
• Standards and compliance
• Migration
• Environmental impacts on the network
Internet of Things

Internet of Things” coined in 1999 associated with RFID

IoT Now: **Standardise IP** into sensors and other objects

Any object or environmental condition can be monitored

Give silent things a voice…(make them **Smart Objects**)

“A pervasive and ubiquitous network which enables monitoring and control of the physical environment by collecting, processing, and analysing the data generated by Smart-Objects”

**Enabling Technologies**

- **Routing Protocol for LLNs (RPL)**
- **Lightweight Protocols**
  - Constrained Application Protocol (COAP)
- **Embedded Network O/S**
  - Contiki uIPv6
- **Open Standards**
  - COAP Simple Management Protocol (CSMP)
IoT Accelerates Digital Transformation

Experience
Deliver Insight for Better Engagement

Productivity
Innovate Easily and Get More Things Done

Monetization
Create New Business and Services

---

**Smartphone Growth (Billions)**

- 2016: 3
- 2020: 4
- 2024: 4.5

Source: IDC; December 2016; Global Smart

**IoT Device Growth (Billions)**

- 2016: 18
- 2020: 31
- 2024: 62

Source: IHS; March 2016; Enabling IoT

---

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Public
IoT Adoption Challenges

- Exponential increase in attack surface
- Automation and Management are critical to managing millions of IoT devices
- How to collect data across diverse device types?
- How to turn data into insight and action?

Open \ Standards based Eco-system is a requirement for business results
IoT Connectivity Characteristics
IoT Ready Digital Network Architecture

Simple
Centralized, policy-based management
Operations-centric visibility and control

Intelligent
Edge application execution
Edge fabric integration

Automated
Plug-and-play deployment
Predictable data delivery

Secure
Visibility – IoT network as a sensor
Context-aware access control
Difference between IoT and Traditional IP Networks

**Bandwidth Constraints**
- x100 less than Wi-Fi (and shared!)

**Highly Unreliable Networks**
- x10^{-12} of error rate on an optical fiber compared to 40% of packet loss!

**Limited resources: power, memory and CPU processing**
- x125k less memory than basic Mac Book!

**Extremely High Scale Network**
- (100’s of millions of devices)
  - e.g., 2M devices for smart metering

---

This is where innovation comes into play with a new vertical agnostic, distributed architecture for the network, and new protocols!
Characteristics of Things?

- These devices are **highly constrained** in terms of
  - Physical size, Inexpensive
  - CPU power, Memory (few tens of kilobytes), Bandwidth (Maximum of 250 KB/s, lower rates the norm)
  - Autonomous operation in the field
- Power consumption is critical
  - If it is battery powered then energy efficiency is paramount, batteries might have to last for years
- May operate in harsh environments
  - Challenging physical environment (heat, dust, moisture, interference)
- Wireless capabilities based on Low Power & Lossy Network (LLNs) technology
  - Predominantly IEEE 802.15.4 (2.4 GHz and 900 MHz)
  - Newer RF technologies IEEE 802.15.4g Smart Utility Network (SUN)
- May also run over wired technologies such as IEEE P1901.2 PLC (Power Line)
- Device Management
  - Installed prior to connectivity
  - Require a level of remote management after deployment
Network Architecture: Potential Impact to the Access Layer

- Centralized, Distributed, and Hybrid topologies
- Access functionality may be divided between critical and non-critical infrastructure
- Critical Infrastructure:
  - Requires Maximum uptime, redundant power, UPS backup (emergency phones, sensors, exit path lighting, etc)
  - Home run to wiring closet
- Non-Critical Infrastructure (no UPS backup requirement)
  - Switch placement in room or in ceiling
High-Level IoT Architecture

Vertical
- IoE Services/Applications

Horizontal
- IoE Middleware
- Core Network
- Industrial
- Consumer
- ...
Common Security Issues in IoT Networks

- Weak Access controls to Monitoring and other equipment
  - Separation of duty for operator, administrator, audit
  - Little or no Password management

- Physical segmentation
  - Dual-homed servers or PLCs act as Firewall
  - Segmented network has only physical security

- Unauthenticated command execution

- Communication is un-encrypted

- Outdated operating systems left unpatched

- Rogue wireless access points without encryption

- Insufficient controls on contractors (i.e. access policy, laptops, etc…)
New Ways to Protect IoE

Threat Intelligence

Cloud-Based Enforcement

Policy/Context | Visibility | Reporting

OpenDNS

New Hardware Platforms

Ruggedized

Industrial

Network Segmentation & Detection

Network as a Sensor

Network as an Enforcer

ALL IoT DEVICES

ALL IoT DEVICES
IoT Based on Open Standards Architecture

- A well proven layered architecture for the IoT, with a migration path for “Legacy” protocols.
- Flexibility and extensibility is KEY

New or emerging protocol for IoT
A World of Proprietary Protocols

• Many legacy networks use **closed and proprietary** protocols
  • Each with different implementations at each layer (Physical, Link, Network)
  • Many **non-interoperable** “solutions” addressing specific problems
  • Resulting in different architectures and protocols

• Interoperability partially addressed (poorly) by protocol gateways
  • Inherently complex to design, deploy and manage
  • Results in inefficient and fragmented networks, QOS, convergence

• Similar situation to computer networks in the 1980s
  • Islands of systems communicating using SNA, IPX, Appletalk, DECnet, VINES
  • Interconnected using multiprotocol gateways
IPv4 or IPv6?

- The current Internet comprises several billion devices
  - Add to this growing 3G, 4G or 5G mobile devices
  - There is no scope for IPv4 to support Smart Object Networks
- Not much IPv4 legacy in Smart Object Networks or LLNs
- Smart Objects will add tens of billions of additional devices
- IPv6 is the only viable way forward
  - Solution to address exhaustion
  - Stateless Auto-configuration thanks to Neighbour Discovery Protocol
- Some issues with IPv6 address size
  - Smart Object Networks use low power wireless with small frame size
  - Solution to use stateless and stateful header compression (6LoWPAN)
What is a Low Power Lossy Network (LLN)?

- LLNs comprise a large number of highly constrained devices (smart objects) interconnected by predominantly wireless links of unpredictable quality

- LLNs cover a wide scope of applications

- Several IETF working groups and Industry Alliance addressing LLNs
  - IETF - CoRE, 6Lowpan, ROLL
  - Alliances - IP for Smart Objects Alliance (IPSO)
Characteristics of LLNs

• LLNs operate with a hard, very small bound on state
• LLNs are optimised for saving energy in the majority of cases
• Traffic patterns can be MP2P, P2P and P2MP flows
• Typically LLNs deployed over link layers with restricted frame-sizes
  • Minimise the time a packet is enroute (in the air/on the wire) hence the small frame size
  • The routing protocol for LLNs should be adapted for such links
• LLN routing protocols must consider efficiency versus generality
  • Many LLN nodes do not have resources to waste
What is 6LoWPAN? (RFC 6282)

- IPv6 over Low power Wireless Personal Area Networks
  - Initially an adaptation layer for IPv6 over IEEE 802.15.4 links
  - Now used by IEEE P1901.2 (PLC), Bluetooth Low Energy, DECT ULE

- Why do we need an adaption layer?
  - IEEE 802.15.4 MTU originally 127 bytes, IPv6 minimum MTU is 1280 bytes
  - Even though 15.4g enables larger frame size, bandwidth optimization is still required
  - IPv6 does not do fragmentation, left to end nodes or lower layers

- Performs 3 functions each with its own 6LoWPAN header
  - IPv6 Header compression
  - IPv6 packet fragmentation and re-assembly
  - Layer 2 forwarding (also referred to as mesh under)

- RFC4919 - Overview, Assumptions, Problem Statement, and Goals
- Cisco SmartGrid endpoints implement RFC 6282 (obsoletes RFC 4944)
6LoWPAN Header Stacks

- Several 6LoWPAN headers are included when necessary
  - IPv6 compression header
  - Fragmentation header (eliminated if single datagram can fit entire IPv6 payload)
  - Mesh or Layer 2 forwarding header (currently not used/implemented)

<table>
<thead>
<tr>
<th>Scenario</th>
<th>IPv6 Frag</th>
<th>Multiple L2 Hops</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.15.4 Header</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>802.15.4 Header</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>802.15.4 Header</td>
<td>Yes</td>
<td>Yes (Future)</td>
</tr>
<tr>
<td>802.15.4 Header</td>
<td>No</td>
<td>Yes (Future)</td>
</tr>
</tbody>
</table>
RPL - Routing Protocol for LLNs

- RPL is an extensible proactive IPv6 distance vector protocol
  - Developed for mesh routing environments
  - Builds a Destination Oriented Directed Acyclic Graph (DODAG) based on an objective
  - RPL supports shortest-path constraint based routing applied to both links and nodes
  - Supports MP2P, P2MP and P2P between devices (leaves) and a root (border router)

- RPL specifically designed for “Lossy” networks
  - Agnostic to underlying link layer technologies (802.15.4, PLC, Low Power Wireless)

- RFC 6550: RPL: IPv6 Routing Protocol for LLNs
- RFC 6551: Routing Metrics Used for Path Calculation in LLNs
- RFC 6552: Objective Function Zero for the Routing Protocol for LLNs
- RFC 6553: RPL Option for Carrying RPL Information in Data-Plane Datagrams
- RFC 6554: An IPv6 Routing Header for Source Routes with RPL
Sample questions

IoT standards

Which option best describes RPL?

A. RPL stands for Routing over Low-power Lossy Networks that use link-state LSAs to determine the best route between leaves and the root border router.

B. RPL stands for Routing over Low-power Lossy Networks that use distance vector DOGAG to determine the best route between leaves and the root border router.

C. RPL stands for Routing over low priority links that use link-state LSAs to determine the best route between two root border routers.

D. RPL stands for Routing over low priority links that use distance vector DOGAG to determine the best route between two border routers.
Learning Matrix for IoT Domain

Cisco Press Books – Suggested Reading
- IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things

Cisco Courses
- Managing Industrial Networks with Cisco Networking Technologies (IMINS)
- Networking Fundamentals for Industrial Control Systems (INICS)
- Control Systems Fundamentals for Industrial Networking (ICINS)

Cisco IoT Webinars

Other References
- IoT Study Guides - https://learningnetwork.cisco.com/docs/DOC-31004
How to stay up to date?
CCIE Community Events

- Interactive online events
- Learning@Cisco leaders discuss state of the industry, program updates, and items that are top of mind to community
- Events held twice a year and are invite-only

https://learningnetwork.cisco.com/community/archived_events/ccie-community-events
CCIE Technical Webinar Series
Technical Sessions focused on new technologies

CISCO DNA DEEP DIVE
DO IT WITH DEVOPS
STEALTHWATCH LEARNING NETWORKS

SELF-LEARNING NETWORKS
OPENSTACK 101
OPENSTACK NEUTRON DEEP DIVE

https://learningnetwork.cisco.com/community/archived_events/ccie-community-events
Stay Connected!
Opt-In for CCIE Specific Information

cisco.com/go/ccie-comms
Cisco Certifications SME Recruitment Program

Collaborate and network with other engineers

Directly influence Cisco Career Certifications (Design, Author, Review)

Use and sharpen technical expertise

Give back to community

Join creativity with experience, knowledge and skills

Experience with assessment techniques

[cisco.com/go/certsme](https://cisco.com/go/certsme)

SME= Subject Matter Expert
Cisco DevNet

- DevNet Sandbox
- Coding 101

https://developer.cisco.com

A Developer Program, providing tools that help you to produce Cisco-enabled applications to sell to Cisco customers, and/or use Cisco APIs to enhance or manage your existing Cisco network.
Complete Your Online Session Evaluation

• Give us your feedback to be entered into a Daily Survey Drawing. A daily winner will receive a $750 gift card.

• Complete your session surveys through the Cisco Live mobile app or on www.CiscoLive.com/us.

Don’t forget: Cisco Live sessions will be available for viewing on demand after the event at www.CiscoLive.com/Online.
Continue Your Education

• Demos in the Cisco campus
• Walk-in Self-Paced Labs
• Lunch & Learn
• Meet the Engineer 1:1 meetings
• Related sessions
Thank you