ARCH (DESIGNING CISCO NETWORK SERVICE ARCHITECTURES) 3.0

Objetivo

Designing Network Service Architectures (ARCH) é um curso que apresenta o projeto de roteamento interno, roteamento BGP, WAN, conectividade para Data Center, segurança, QoS, transição para IPv6 e Multicast. Esse curso habilita o aluno para projetar redes que cumpra os requerimentos especificados pelo cliente, em segurança, eficiência, com alta disponibilidade e escalabilidade. Após completar este treinamento o aluno estará apto à: • Projetar conectividade com alta disponibilidade em rede corporativa (Enterprise); • Projetar conectividade utilizando BGP em redes corporativas (Enterprise); • Projetar conectividade WAN em redes corporativas (Enterprise); • Projetar a integração com Data Center em redes corporativas (Enterprise); • Projetar serviços de segurança em redes corporativas (Enterprise); • Projetar serviços de QoS para otimizar a experiência dos usuários; • Projetar a transição para soluções em IPv6; • Projetar redes Multicast em redes corporativas (Enterprise).

Público Alvo

O público inclui os profissionais em pré-vendas e pós-vendas que trabalham em projetos de soluções de redes corporativas (Enterprise), abrangendo projeto, planejamento e implantação. Os profissionais em pós-vendas envolvidos na implantação podem fornecer subsídios essenciais para os profissionais em pré-vendas para a correção de possíveis desvios entre o projeto e a real solução. Esse curso é também preparatório para os profissionais que buscam a certificação CCDP (Cisco Certified Design Professional).

Pré-Requisitos

Os conhecimentos necessários para um excelente aproveitamento deste curso são: Descrever e aplicar metodologias para projetos de redes; Descrever e aplicar conceitos em modularidade e hierarquia em projetos de redes; Projetar redes considerando resiliência e escalabilidade entre os componentes; Projetar conectividade para integração com internet e roteamento interno; Integrar soluções em colaboração e redes sem fio (Wireless); Projetar soluções em endereçamento IPv4 e IPv6; Operação em redes com múltiplos switches, configurando vlans, links troncos (trunk), STP (spanning-tree), DHCP e links agregados (Port Aggregation); Configurar e fornecer suporte em roteamento IPv4 e IPv6 em redes corporativas (rotas estáticas, protocolos EIGRP, OSPF multi-área e RIPng); Implantar conectividade internet para redes corporativas (rotas estáticas e BGP básico); Implantar mecanismos em redistribuição e filtragem de rotas; Implantar políticas para controle de seleção de caminhos (Policy Based Routing e IP SLA); Implantar redundâncias em ambientes IPv4 e IPv6 (First Hop Redundancy); Configurar equipamentos para processo SNMP, Syslog e NetFlow; Utilização das melhores práticas recomendadas em segurança. Recomendado o aluno ter participado ou possuir conhecimentos equivalentes abrangidos pelos cursos SWITCH v2.0, ROUTE v2.0, TSHOOT v2.0 e DESGN v3.0.

Carga Horária

40 horas (5 dias).

Conteúdo Programático

Course Introduction
Overview
Course Goal and Objectives
Course Flow
Additional References

Enterprise Connectivity and High-Availability

EIGRP Design Considerations
Scaling EIGRP Designs
EIGRP Fast Convergence
EIGRP with Multiple Autonomous Systems
Reasons for Multiple EIGRP Autonomous Systems
Bidirectional Forwarding Detection
EIGRP Graceful Restart/NSF Fundamentals
EIGRP Hierarchical Design Basics
Creating Choke Points
EIGRP Two-Layer Hierarchy
EIGRP Three-Layer Hierarchy
EIGRP Hub and Spoke Design
Summarization Challenges: Black Holes
Summarization Challenges: Suboptimal Routing
EIGRP Hub and Spoke Scaling
EIGRP Stub Leaking
Case Study: EIGRP DMVPN
EIGRP DMVPN Scaling

OSPF Design Considerations
Factors Influencing OSPF Scalability
OSPF Scalability: Adjacent Neighbors
Routing Information in the Area and Domain
OSPF Scalability: Routers in an Area
OSPF Scalability: Areas per ABR
Designing Areas
OSPF Hierarchy
Area and Domain Summarization
OSPF Full Mesh Design
OSPF Hub-and-Spoke Design
OSPF Hub-and-Spoke ABR Placement
Number of Areas in OSPF Hub-and-Spoke Design
OSPF Hub-and-Spoke Network Types
Improving OSPF Convergence
Bidirectional Forwarding Detection
OSPF Event Propagation
OSPF Event Processing
OSPF Flood Reduction

OSPF Database Overload Protection

IS-IS Design Considerations
Overview of IS-IS
IS-IS Hierarchical Design
IS-IS Router and Link Types
IS-IS Adjacencies
Integrated IS-IS Routing
Similarities Between IS-IS and OSPF
OSPF and IS-IS Characteristics
Integrated IS-IS vs. OSPF: Area Design
Case Study: IS-IS Addressing
IS-IS Packets
IS-IS Information Data Flow
Case Study: IS-IS Routing Logic
Route Leaking
Route Leaking Loop Prevention
Asymmetric vs. Symmetric IS-IS Routing
IS-IS Network Types
IS-IS Operations
IS-IS LSP Flooding
IS-IS LSDB Synchronization
IS-IS Design Considerations
IS-IS Summarization
Integrated IS-IS for IPv6
IS-IS Single Topology Restrictions
Multitopology IS-IS for IPv6

BGP Design

Designing IBGP Sessions
IBGP Scalability Issues
IBGP Scalability Solution: Route Reflectors
BGP Route Reflector Definitions
IBGP Scalability Solution: Confederations
Comparing BGP Confederations to BGP Route Reflectors
BGP Split-Horizon Rule
Route Reflector Split-Horizon Rule
BGP Split-Horizon Rules: Refresher
Redundant Route Reflectors
Route Reflector Clusters
Route Reflector Clusters: Cluster ID
Additional Loop-Prevention Mechanisms
Loop-Prevention: Cluster-List
Network Design with Route Reflectors
Hierarchical Route Reflector Design
Potential Network Issues

Designing BGP Communities
Single-Homing vs Multi-Homing
Dual-Homing and Multi-Homing Design Considerations
Load Sharing: Single-Homed, Multiple Links
Load Sharing: Dual-Homed to One ISP, Single Local Router
Load Sharing: Dual-Homed to One ISP, Multiple Routers
Load Sharing: Multihoming with Two ISPs, Single Local Router
Load Sharing: Multihomed, Two ISPs, Multiple Local Routers

Wide Area Networks Design

Service Provider Managed VPNs
Choosing Your WAN Connection
Layer 3 MPLS VPN
MPLS/VPN Architecture
PE Router Architecture
Route Distinguishers
Route Targets
Using EIGRP as the PE-CE Routing Protocol
Using OSPF as the PE-CE Routing Protocol
Using BGP as the PE-CE Routing Protocol
Case Study: MPLS/VPN Routing Propagation
Forwarding in MPLS VPN
VPWS Overview
VPWS Design
VPLS Design
VPLS vs. VPWS

Enterprise Managed VPNs
Enterprise Managed VPNs Overview
GRE Overview
Multipoint GRE Overview
IPsec Overview
IPsec and GRE
IPsec and Virtual Tunnel Interface
IPsec and Dynamic VTI
GETVPN
DMVPN Overview
DMVPN Phase 1
DMVPN Phase 2
DMVPN Phase 3
Case Study: MPLS/VPN over GRE/DMVPN
DMVPN and Redundancy
SSL VPN Overview
FlexVPN Overview
FlexVPN Architecture
FlexVPN Capabilities
FlexVPN Configuration Blocks

WAN Resiliency Design
WAN Remote-Site Overview
Common MPLS WAN Design Models
Common Layer 2 WAN Design Models
Common VPN WAN Design Models
3G/4G VPN Design Models
Remote-Site Using Local Internet
Remote-Site LAN
Case Study: Redundancy and Connectivity Use Cases
Basic Traffic Engineering Techniques
IWAN Solution Overview
Intelligent WAN Design Overview
IWAN Hybrid Design Model
Cisco PfR Overview
Cisco PfR Versions
Cisco PfR Operations
Multisite Cisco PfR
Cisco PfR Design and Deployment Considerations

Campus Edge and Connectivity to Partners
Case Study: Campus Edge
Challenges of Connecting External Partners
Extranet Topology—Remote LAN Model
Extranet Topology—Interconnect Model
Security and Multitenant Segmentation

SDN and APIC-EM
SDN Overview
SDN Challenges
Direction of Nontraditional SDN
SDN Requirements
Cisco SDN Solutions
Enterprise WAN and Access Management
Cisco ONE: APIC-EM
Design APIC-EM
SDN Security Challenges
SDN Security: DC and EM

Enterprise Data Center Integration

Modular and Scalable Data Center Network
Case Study: Connecting Servers to Enterprise LAN
Case Study: 2-Tier Data Center Network Architecture
Case Study: 3-Tier Data Center Network Architecture
Data Center Inter-VLAN Routing
End of Row vs. Top of Rack Design
Fabric Extenders
Case Study: Data Center High-Availability

Network Interface Controller Teaming
Cisco FabricPath
Overlay Networking in Data Center

Multi-Tenant Data Center
Multi-Tenant Data Center Overview
Secure Tenant Separation
Layer 3 Separation with VRF-Lite
Virtual Device Contexts
Case Study: Multi-Tenant Data Center
Micro-Segmentation with Overlay Networks

Data Center Interconnections
Need for DCI
IP Address Mobility
Case Study: Dark Fiber DCI
Pseudowire DCI
Virtual Private LAN Service DCI
Any Transport over MPLS over GRE
Layer 2 DCI Caveats
Overlay Transport Virtualization DCI
Overlay Networking DCI

Data Center Traffic Flows
Traffic Flow Directions
Traffic Flow Types
Case Study: Separation of Application Tiers
Securing East-West Traffic

SDN and APIC-DC
Application Centric Infrastructure Data Center
Cisco ACI Fabric
Network Virtualization Overlays
Design Applications Using Cisco ACI
Design EPGs
Designing Applications
Application Network Profile Discovery
Application Network Profile Discovery—Unknown Applications

Design Security Services

Security Services Overview
Network Security Zoning
Cisco Modular Network Architecture
Cisco Next-Generation Security

Designing Infrastructure Protection
Cisco Network Infrastructure Protection
Infrastructure Device Access
Secure Management Access
Routing Infrastructure
Device Resiliency and Survivability
Network Policy Enforcement
Switching Infrastructure

Designing Firewall and IPS Solutions
Firewall Architectures
Case Study: Implementing Firewall in Data Center
Virtualized Firewalls
Case Study: Firewalls High Availability
IPS Architectures
IPS High Availability

Designing Network Access Control Solutions
IEEE 802.1X Overview
Case Study: Authorization Options
IEEE 802.1X Phased Deployment
Extensible Authentication Protocol
802.1X Supplicants
Cisco TrustSec

Design QoS for Optimized User Experience

QoS Overview
IntServ vs. DiffServ
Classification and Marking Tools
Layer 2 Marking: IEEE 802.1Q/p Class of Service
Layer 3 Marking: IP Type of Service
Layer 3 Marking: DSCP Per-Hop Behaviors
Layer 2.5 Marking: MPLS Experimental Bits
Mapping QoS Marking Between OSI Layers
Layer 7 Classification: NBAR/NBAR2
Policers and Shapers
Token Bucket Algorithms
Policing Tools: Single-Rate Three-Color Marker
Policing Tools: Two-Rate Three-Color Marker
Queuing Tools: Overview
Queuing Tools: Tx-Ring
Queuing Tools: Fair-Queuing
Queuing Tools: CBWFQ
Queuing Tools: LLQ
Dropping Tools: DSCP-Based WRED
Dropping Tools: IP ECN

Recommended QoS Design Principles
Classification and Marking Design Principles
Policing and Remarking Design Principles
Queuing Design Principles
Dropping Design Principles
Per-Hop Behavior Queue Design Principles
RFC 4594 QoS Recommendations
QoS Strategy Models
4-Class QoS Strategy
8-Class QoS Strategy
12-Class QoS Strategy

Campus QoS Design
Why Do We Need QoS in Campus?
VoIP vs. Video
Buffers and Bursts
Trust States and Boundaries
Trust States and Boundaries Example
Dynamic Trust State
Classification/Marking/Policing QoS Model
Queuing/Dropping Recommendations
EtherChannel QoS Design
Example: Campus QoS Design

Data Center QoS Design
Need for QoS in Data Center
Example: High Performance Trading Architecture
Example: Big Data Architecture
Example: Virtualized Multiservice Architectures
Data Center Bridging Toolset
Example: DC QoS Application

WAN QoS Design
Need for QoS in MPLS VPN
L2 Private WAN QoS Administration
Fully Meshed MPLS VPN QoS Administration
MPLS DiffServ Tunneling Modes
Example: MPLS VPN QoS Roles

IPsec VPN QoS Design
Need for QoS in IPsec VPN
VPN Use Cases and Their QoS Models
IPsec Refresher
IOS Encryption and Classification Order of Operations
MTU Considerations
DMVPN QoS Considerations
GET VPN QoS Considerations

Transition to IPv6

Deploying IPv6
IPv6: Why?
IPv6 Phased Approach
IPv6 Phased Approach: Business and Network Discovery Phase
IPv6 Phased Approach: Assessment
IPv6 Phased Approach: Planning and Design
IPv6 Phased Approach: Implementation and Optimization
First Steps Towards IPv6
Provider Independent vs. Provider Assigned
Where to Start the Migration
IPv6 Islands
IPv6 WAN
Transition Mechanisms
NAT64 and DNS64
Manual Tunnels
Tunnel Brokers
6 Rapid Deployment
DS-Lite
LISP
Dual-Stack

Challenges with Transition to IPv6
IPv6 Services
Link Layer Security Considerations
Application Support
Application Adaptation
Application Workarounds
Control Plane Security
Dual Stack Security Considerations
Tunneling Security Considerations
Multihoming

Design Enterprise IPv6 Network
Design Transition to IPv6

IP Multicast Design

Defining Multicast Distribution Trees and Forwarding
How Does IP Multicast Work?
Multicast Group
IP Multicast Service Model
Functions of a Multicast Network
Multicast Protocols
Multicast Forwarding and RPF Check
Case Study: RPF Check Fails and Succeeds
Multicast Protocol Basics

Multicast Distribution Trees Identification

Introducing PIM-SM Protocol and PIM-SM Enhancements
PIM-SM Overview
Receiver Joins PIM-SM Shared Tree
Source Is Registered to RP
PIM-SM SPT Switchover
Multicast Routing Table
Basic SSM Concepts
SSM Scenario
Bidirectional PIM
PIM Modifications for Bidirectional Operation
DF Election
DF Election Messages
Case Study: DF Election

Rendezvous Point Distribution Solutions
Rendezvous Point Discovery
Rendezvous Point Placement
Auto-RP
Auto-RP Candidate RPs
Auto-RP Mapping Agents
Auto-RP Other Routers
Case Study: Auto-RP Operation
Auto-RP Scope Problem
PIMv2 BSR
PIMv2 BSR—Candidate RPs
PIMv2 BSR—Bootstrap Router
PIMv2 BSR—All PIMv2 Routers
BSR Flooding Problem
IPv6 Embedded Rendezvous Points
Anycast RP Features
Anycast RP Example
MSDP Protocol Overview
MSDP Neighbor Relationship
Case Study: MSDP Operation

IP Multicast Security
Multicast Security Challenges
Problems in the Multicast Network
Multicast Network Security
Network Element Security
Security at the Network Edge
Securing Auto-RP and BSR
Internal Multicast Security
Sender Control
Receiver Control
Admission Control

MSDP Security

Labs
Challenge 1: Design Enterprise Connectivity
Challenge 2: Design Enterprise BGP Network with Internet Connectivity
Challenge 3: Design Resilient Enterprise WAN
Challenge 4: Design Enterprise Data Center Connectivity
Challenge 5: Design Secure Enterprise Network
Challenge 6: Design QoS in Enterprise Network
Challenge 7: Design Enterprise IPv6 Network