DESGN (DESIGNING FOR CISCO INTERNETWORK SOLUTIONS)

Objetivo

Designing For Cisco Intertwork Solutions (DESGN) é um curso que apresenta o processo modular e estruturado para o estabelecimento de projetos escaláveis, resilientes e com domínios de disponibilidade definidos. Esse curso apresenta projetos para soluções em roteamento e comutação (switching) para redes LAN Campus e Empresariais (Enterprise) em detalhes. Também são apresentados em abordagem introdutória a integração de soluções de Data Center, Redes Sem Fio (Wireless) e de infraestrutura para tráfegos em tempo real (real-time), abordando e seus efeitos e impactos no núcleo da rede (Camada Core), sob a ótica e perspectiva de projetos. Esse curso habilita o aluno em reunir e estabelecer os requerimentos em redes de comunicação para clientes, identificando soluções, para o estabelecimento de soluções em infraestrutura, para garantir as funcionalidades básicas para o propósito final do projeto. Após completar este treinamento o aluno estará apto à: • Descrever e aplicar metodologias em projetos de redes; • Descrever e aplicar conceitos de modularidade e hierarquia em projetos de redes; • Projetar Redes LAN Campus resilientes e escaláveis; • Projetar soluções de conectividade resilientes e escaláveis entre seções de redes empresariais; • Projetar conectividade para a internet e roteamento interno em uma rede; • Integrar soluções em colaboração e redes sem fio no núcleo da rede; • Estruturar endereçamento escalável para a rede (IPv4 e IPv6); • Descrever em abordagem introdutória soluções SDN (Software Defined Networks).

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 CCDA (Cisco Certified Design Associate).

Pré-Requisitos

Os conhecimentos necessários para um excelente aproveitamento deste curso são: 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 e TSHOOT v2.0.

Carga Horária

40 horas (5 dias).

Conteúdo Programático

Course Introduction
Overview
Course Goal and Objectives
Course Flow
Additional References

Design Methodologies

Design Life Cycle
Business-Driven Network
Plan, Build, Manage
Plan Phase
Build Phase
Manage Phase
Project Deliverables

Characterizing Existing Network
Why Is Good Characterization Necessary?
Steps of Gathering Information
Auditing the Existing Network
Using Tools to Characterize Existing Network
Case Study: Using SNMP to Gather Information
Case Study: Using NetFlow to Gather Information
Case Study: Using CDP or LLDP to Gather Information
Document the Existing Network

Top-Down Approach
Top-Down vs. Bottom-Up
Benefits and Drawbacks of Top-Down Approach
Case Study: Top-Down Approach Design
Pilots and Prototypes

Network Design Objectives

Building a Modular Network

Network Convergence
Why Would You Modularize?
How to Modularize?
Where Should You Hide Information?
Amount of Information Hiding
Modularity and Fault Domains
How Scalability Can Be Achieved Through Modular Design
How Resiliency Is Achieved Through Modular Design
Case Study: Modular Network Design
Typical Enterprise Network Modules

Applying Modularity: Hierarchy in a Network
Hub-and-Spoke Design
Three-Layer Hierarchy
Access Layer
Distribution Layer
Core Layer
Two-Layer Hierarchy
Multilayer Hierarchy

Applying Modularity: Virtualization Overview
What Is Virtualization?
Reasons for Virtualization
Types of Virtualization
Consequences of Virtualization

Campus Network Design

Layer 2/Layer 3 Demarcation
End-to-End vs. Local VLANs
Traditional Layer 2 Access Layer
Updated Layer 2 Access Layer
Layer 3 Access Layer
Routed or Switched Access Layer?
Hybrid Access Layer
Case Study: Common Access-Distribution Interconnection Designs
Small and Medium Campus Design Options

Layer 2 Design Considerations
VLAN and Trunk Considerations
VTP Considerations
STP Considerations
STP Root Bridge Placement
Alignment of STP with FHRP
Consistent STP Metrics
Cisco STP Toolkit
STP Stability Mechanism Recommendations
Problem with Unidirectional Links

Comparing Loop Guard with UDLD
UDLD Recommended Practices
Need for MST
MST Recommended Practices

High Availability Considerations
Managing Bandwidth and Oversubscription
Port Aggregation Considerations
VSS Considerations
Stacking Considerations
First Hop Redundancy
HSRP/VRRP Subsecond Failover
HSRP/VRRP Preempt Delay
HSRP/VRRP Load Sharing
HSRP/VRRP Tracking
Case for GLBP
Case Against GLBP

Layer 3 Design Considerations
Building Triangles
Redundant Links
Routing Convergence
Limit Peering Across the Access Layer
Summarize at Distribution Layer

Traffic and Interconnections
Network Requirements of Applications
Client-Server Traffic Considerations
Intrabuilding Structure Considerations
Interbuilding Structure Considerations
Transmission Media Considerations
Case Study: Transmission Media

Enterprise Network Design

Designing a Secure Network
Key Threats in Campus
Security Goals
Securing the Perimeter
Introduction to Firewalls
Flavors of Firewalls
Firewall Recommended Practices
IPS/IDS Fundamentals
IPS/IDS Recommended Practices
Network Access Control
Security Implications of Client Access Methods

Edge Connectivity Design
Edge Overview
DMZ Overview
DMZ Segmentation
DMZ Service Placing
Internet Connectivity
Internet Edge with High Availability
VPN Design
Site-to-Site VPN Use Cases
Overview of Remote Access Flavors
Security Services Design
Edge Device Selection
NAT Placement

WAN Design
WAN Topologies
How Should I Connect Remote Sites?
WAN Considerations
Provider-Managed VPNs: Layer 2 vs. Layer 3
MPLS Overview
Layer 3 VPN: MPLS/VPN
Layer 3 VPN: MPLS/VPN Considerations
Layer 2 VPN: VPWS
Layer 2 VPN: VPWS Considerations
Layer 2 VPN: VPLS
Layer 2 VPN: VPLS Considerations
Provider-Managed VPNs: Making Choices
Introducing Enterprise-Managed VPNs
Deploying Enterprise-Managed VPN over Provider-Managed VPN
IPsec Overview
Enterprise-Managed VPN: IPsec Tunnel Mode
Enterprise-Managed VPNs: GRE over IPsec
Enterprise-Managed VPNs: DMVPN
Enterprise-Managed VPNs: IPsec VTI
Enterprise-Managed VPNs: GETVPN
Enterprise-Managed VPNs: Making Choices

Branch Design
Branch Putting Pressure on the WAN
Common Branch Connectivity Options
Branch Redundancy Options
Single-Carrier WANs vs. Dual-Carrier WANs
Single-Carrier MPLS/VPN Site Types
Dual-Carrier MPLS/VPN WAN
Hybrid WAN: Layer 3 Provider VPN and IPSec VPN
Hybrid WAN: Layer 2 Provider VPN and IPSec VPN
Branch Internet Access—Centralized or Local?

Remote-Site LAN: Flat Layer 2
Remote-Site LAN: Collapsed Core

Connecting to the Data Center
Data Center Architecture
Data Center Ethernet Infrastructure
Data Center Storage Integration
Data Center Reference Architecture
Server Virtualization and Virtual Switch
Resilient Data Center Core Options
Data Center Security
Need to Connect Data Centers
Data Center Interconnect Options
Extending Layer 2 Between Data Centers
Supporting Server Scalability
Application-Level Load Balancing
Network-Level Load Balancing

Design of Internal Routing and Connecting to the Internet

Routing Protocol Considerations
Interior and Exterior Routing Protocols
Route Summarization
Originating Default Routes
Route Redistribution
Avoiding Transit Traffic
Defensive Filtering
Use Cases for Passive Interfaces
Routing Protocol Fast Convergence
Coexistence of IPv4 and IPv6 IGP Routing
Routing Protocol Authentication

Expanding EIGRP Design
Case Study: Single-Homed Site
Case Study: Dual-Homed Site
Case Study: Geographic Dispersion of HQ
Case Study: Stub Feature
Case Study: Summarizing Towards the Core

Expanding OSPF Design
Case Study: OSPF Areas
Review of OSPF LSAs
Case Study: OSPF Summarization
Case Study: OSPF Path Selection
Case Study: OSPF Stubby Areas Case Study: Single-Homed Site

Introducing IS-IS
Introducing IS-IS

IS-IS Areas
Inter-Router Communication
CLNS Addressing
IS-IS Metric
IS-IS Load Balancing
IS-IS Authentication
Basic IS-IS Configuration
IS-IS for IPv6

Expanding IS-IS Design
Area and Scaling
IS-IS Hub-and-Spoke Scaling
Case Study: IS-IS Hub-and-Spoke

Using BGP to Connect to the Internet
Case Study: Single and Dual-Homing
Case Study: Multihoming
Implications of Running Full BGP Routing Table
Running a Partial Internet Table
BGP Route Selection Process
Influencing Outbound and Inbound Routing
Influencing Outbound Routing: Weight Attribute
Influencing Outbound Routing: Local Preference
Influencing Inbound Routing: Setting MED Outbound
Influencing Inbound Routing: Setting Communities Outbound
Influencing Inbound and Outbound Routing: Prepending AS Path
Case Study: Avoiding Loops When Forwarding to the Internet
Route Dampening
Coexistence of BGP for IPv4 and IPv6

Expanding the Existing Network

Understanding Quality of Service
Traffic Characteristics
Need for QoS
QoS Mechanisms Overview
Trust Boundary
QoS Mechanisms – Classification and Marking
Classification Tools
QoS Mechanisms – Policing, Shaping, and Re-Marking
Tools for Managing Congestion
Tools for Congestion Avoidance
QoS Deployment Principles
Recommended Practice QoS Design Principles
Design Strategies

Supporting Wireless Access
Introduction to Wireless LAN Networks

Autonomous WLAN Architecture
Centralized WLAN Architecture
Speciality WLAN Architecture: Wireless Bridge
Cloud-Enabled WLAN Architecture
LAN Bandwidth Considerations
Trunk and VLAN Configuration
WLAN and PoE
WLAN and End-to-End QoS
Supporting Wireless Security
Integrating Collaboration
Collaboration Overview
Collaboration Building Blocks
Supporting IP Telephony
Voice VLAN
Protocols of IP Telephony
Collaboration Traffic
Traffic Patterns
Assuring Good User Experience

IP Addressing Design

Concepts of Good IP Addressing
IP Addressing Goals
Planning IP Addressing
Planning Addressing for the Future
Route Summarization with IPv4
Route Summarization with IPv6
Public and Private Addressing
Avoiding Re-Addressing

Creating an Addressing Plan for IPv4
Planning the IP Addressing Hierarchy
Creating an Addressing Plan
Case Study: IPv4 Address Space
Case Study: Resolving Overlapping Address Ranges
Allocating More IP Addresses
Voice Overlay Subnets
Need for Loopbacks

IPv6 Addressing
Benefits and Challenges of IPv6 Addressing
Structure of an IPv6 Address
IPv6 for an Enterprise
IPv6 Address Allocation: Linked IPv4 Into IPv6
IPv6 Address Allocation: Per Location/Type
Case Study: Location-Based Subnetting
Case Study: Type-Based Subnetting
IPv6 Address Allocation: Per VLAN

IPv4 and IPv6 Coexistence

Supporting IP Addressing
IP Address Management
IPv4 Address Assignment Recommended Practices
IPv6 Address Assignment Recommended Practices
DNS Recommended Practices
Case Study: DHCP and DNS Servers in a Network

Introduction to Software Defined Networks

SDN Overview
SDN Definition
Need for SDN
Path to Network Programmability
SDN Flavors
SDN Framework
SDN Controllers
Southbound APIs
Northbound APIs
OpenFlow
OpenDaylight
Cisco ACI

Labs
Challenge 1: Ask the Right Questions
Challenge 2: Design Branch's LAN
Challenge 3: Design Branch’s Connections to the HQ
Challenge 4: Design Branch’s Routing
Challenge 5: Design Support for Wireless and Collaboration
Challenge 6: Design IPv4 Addressing Plan
Challenge 7: Design IPv6 Addressing Plan