Ingram Micro Training Center Catalog

trening-serbia@ingrammicro.com

1. Check Point

1.1. Check Point Certified Security Administrator (CCSA)
1.2. Check Point Certified Security Expert (CCSE)
1.3. Certified Troubleshooting Administrator (CCTA)
1.4. Check Point Troubleshooting Expert (CCTE)
1.5. Harmony Endpoint Specialist (CCES)
1.6. Cybersecurity Boot Camp (CCSA & CCSE)

2. Radware

2.1. Radware Alteon Level 1
2.2. Radware DefensePro level 1
2.3. Radware Alteon Secure (AppWall)

3. VMware

3.1. Vmware vSphere: Install, Configure, Manage V8

4. Veritas

4.1. Veritas NetBackup 8.2: Administration
4.2. NetBackup 8.2: Advanced Administration

5. Veeam

5.1. Veeam Backup & Replication v12.3 Configure, Manage, Recover

6. Customized Trainings

6.1. Cisco:

6.1.1. Cisco Umbrella Deployment and Configuration
6.1.2. Cisco Secure Access by Duo Training
6.1.3.Cisco Meraki Solutions
6.1.4. Cisco Enterprise Advanced Routing and Services (ENARSI)
6.1.5. Implementing and Operating Cisco Enterprise Network Core Technologies (ENCOR)
6.1.6. Implementing and Administering Cisco Solutions (CCNA)
6.1.7. Cisco Secure Email Gateway Bootcamp
6.1.8. Cisco Firepower Bootcamp
6.1.9. Webex Calling Technical Bootcamp
6.1.10. Cisco/Viptela SD-WAN Bootcamp
6.1.11. Cisco ISE Fundamentals
6.1.12. Wi-Fi Fundamentals

6.2. IBM:

6.2.1. Introduction to Basic AI concepts and IBM AI Tools and Models
6.2.2. IBM watsonx.ai Technical Sales Workshop (L3 labs)
6.2.3. IBM watsonx.ai Technical Workshop (L4 Labs)
6.2.4. IBM watsonx.data Technical Sales Workshop

6.3. Juniper:

6.3.1. Introduction to Juniper world & Junos
6.3.2. Introduction to Juniper Mist AI
6.3.3. Juniper AI-driven Enterprise (AIDE)
6.3.4. Juniper Intent-Based Data Center Fundamentals
6.3.5. Securing Your Juniper Networks
6.3.6. Advanced BGP For Service Providers
6.3.7. Introduction To Junos OS – one-day Essentials
6.3.8. Implementing Data Center Fabric With EVPN and VXLAN
6.3.9. Junos Enterprise Switching - One day Essentials

Check Point Certified Security Administrator (CCSA)

Course Overview

Check Point Certified Security Administrator (CCSA) R81.20 is a three-day training aimed at technical personnel and covers the installation, setup and management of Check Point Software solutions. The goal of the course is to understand the basic concepts and acquire the skills necessary for the configuration of Check Point Firewall and Check Point Management.

Prerequisites

Basic knowledge of TCP/IP Knowledge of the basics of Windows and UNIX, network services and the use of the Internet

CHECK POINT PLATINUM ATC PARTNER 2024 CONTRIBUTION

INGRAM MICRO® | Trening Centar Beograd

DAY 01

Understanding the concept of Firewall and understanding the mechanisms used to control traffic flow;

Describing the most important elements of the Check Point Unified Security Management Architecture;

Getting to know SmartConsole features, functions and tools;

Understanding the application of Check Point solutions;

Describing the basic functions of Gaia;

Describing the basic elements of Security Policy;

Understanding Unified Security Policy traffic inspection;

DAY 02

The role of the Administrator in the creation of Management

Backup techniques;

Concepts of Layer Policy;

Recognition and understanding of Check Point security solutions and products, and how they work to protect

Licensing of Check Point solutions;

Using tools designed to monitor data, find threats and improve performance;

Using tools designed for quick response and efficient changes to Firewall, tunnels, remote; Users, traffic flow and other activities;

Understanding Site-to-Site and Remote Access VPNs;

DAY 03

Analysis and interpretation of VPN traffic;

Defining Users and User Groups;

Access management of all Users;

The basics of ClusterXL technology and the benefits of using it;

Periodic Administration;

LAB OUTLINE:

Working with Gaia;

Modification of Existing Security Policies;

Configuration of Dynamic and Static NAT;

Admin Access Control;

Installation and Remote Firewall Management;

Backup;

Defining an Access Control Policy;

Defining the Security Policy;

Licensing;

Working with Check Point Logs;

Site-to-Site VPN configuration;

Providing Access to Users;

Working with ClusterXL;

Network Compliance Verification;

Working with CP View;

CHECK POINT
PLATINUM
ATC PARTNER
2024
CONTRIBUTION

Check Point Certified Security Expert (CCSE)

Course Overview

Check Point Certified Security Expert (CCSE) R81.20 is a training designed for experts who will perform advanced configuration of Check Point Software solutions. The aim of the course is to understand and acquire the skills necessary for the configuration and optimal management of the Check Point Next Generation Firewall.

Prerequisites

CCSA Training/Certificate
Basic knowledge of Windows, UNIX, network systems, TCP/IP and Internet usage

INGRAM MICRO® | Trening Centar Beograd

DAY 01

Advanced CLI commands;

Application of upgrades, patches and hotfixes;

Describing the Check Point Firewall infrastructure;

Advanced methods of centralized log collection using CPView and

Use of Check Point API in flexible system automation;

Advanced ClusterXL functionality;

Advantages of VRRP redundancy;

DAY 02

Advantages and working principle of SecureXL;

Advantages and principle of operation of CoreXL;

SmartEvent components that allow us to archive logs, as well as generate

SmartEvent processes that indicate security breaches on the

Understanding of SmartEvent in order to detect and suppress security

The working principle of Mobile Access
Software Blace and its secure

Installation of Mobile Access;

Check Point solutions for access from a remote location;

DAY 03

Check Point Capsule, its components and principle of operation;

Check Point solutions against cyber attacks, such as Zero-day and Advanced Persistent Threats;

The working principle of SandBlast, Threat Emulation and Threat Extraction in prevention;

Check Point Threat Prevention in the function of preventing the loss of corporate data on smartphones and tablets;

LAB OUTLINE:

Upgrade Security Management Server to R81.20;

Adding Check Point Hotfixes;

Configuring the Cluster;

Advanced CLI Firewall Administration;

Configuring manual NAT;

Creating Objects using the Check Point API;

Configuring Check Point VRRP;

Adding a Secondary Security Management Server;

Viewing the Chain Modules;

Working with SecureXL;

Working with CoreXL;

Identifying threats using SmartEvent;

Use of Mobile Access;

Understanding and configuring IPS;

Configuring Threat Prevention and Threat Protection;

Configuring Threat Emulation and Threat Extraction;

Certified Troubleshooting Administrator (CCTA)

Course Overview

This course is designed for security administrators and Check Point resellers who need to manage and monitor issues that may occur within their Security Management environment. Demonstrate and apply understanding of the concepts and skills necessary to trouble-shoot issues that may occur when managing the Security Management environment.

Prerequisites

Working knowledge of UNIX and/or Windows operating systems. Working knowledge of Networking TCP/IP. CCSA training/certification. Advanced knowledge of Check Point Security products.

Timing & Duration of the training

DAYS

INGRAM MICRO® | Trening Centar Beograd

OBJECTIVES

Identify basic resources available to troubleshoot Check Point Security Gateways and Management Software Blades that run onthe Gaia operating system.

Discuss how to use the OSI (Open Systems Interconnection) model for problem isolation.

Investigate and troubleshoot potential traffic flow issues.

Monitor network activity and performance.

Investigate and troubleshoot log collection issues.

Investigate and trouble-shoot

Investigate and troubleshoot Application Control and URL Filtering issues.

Investigate and troubleshoot NAT (Network Address Translation)

Investigate and troubleshoot issues with basic Site-to-Site VPNs.

Investigate and troubleshoot Autonomous Threat Prevention

Investigate and troubleshoot Licenses and Contracts issues.

EXERCISES

Troubleshoot with Linux and Check Point Commands

Collect and Analyze Interface Packet Captures

Troubleshoot Log Communication Issues

Troubleshoot SmartConsole

Troubleshoot Application Control and URL Filtering

Investigate Network Address Translation Issues

Troubleshoot Site-to-Site VPN

Evaluate Threat Prevention Products

Verify Licenses

Check Point Troubleshooting Expert (CCTE)

Course Overview

This course is designed for security experts and Check Point resellers who desire to obtain the necessary knowledge required to perform more advanced troubleshooting skills while managing their security environments. Provide advanced troubleshooting skills to investigate and resolve more complex issues that may occur while managing your Check Point Security environment.

Prerequisites

Working knowledge of UNIX and/or Windows operating systems; Working knowledge of Networking TCP/IP; CCSE training/ certification; Advanced knowledge of Check Point Security products;

INGRAM MICRO® | Trening Centar Beograd

DAY 01

Advanced Troubleshooting;
Management Database and Processes;
Advanced Kernel Debugging;
User Mode Troubleshooting;

DAY 02

Advanced Access Control
Understanding Threat Prevention
Advanced VPN Troubleshooting
Acceleration and Performance Tuning

LAB OUTLINE:

Monitoring Network Traffic
Debugging Management Processes
Exploring the Postgres and Solr Databases
Troubleshooting Management Synchronization
Analyzing Traffic Issues Using Kernel Debugs
Debugging User Mode Processes
Troubleshooting Application Control and URL Filtering
Troubleshooting IPS ˜ Evaluating Threat Prevention Products
Debugging Site-to-Site VPN ˜ Troubleshooting Remote Access
Testing Mobile Access VPN
Evaluating SecureXL
Modifying CoreXL
Evaluating Hardware-related Performance
Tuning and Software Optimization

Harmony Endpoint Specialist (CCES)

Course Overview

This course is designed for Security Administrators who are responsible for deploying and managing a Harmony Endpoint security solution. Demonstrate an understanding of the Check Point Harmony Endpoint solution, including its features and capabilities. Apply knowledge and skills gained during training to manage and protect a Harmony Endpoint solution.

Prerequisites

Working knowledge of Unix-like and/or Windows operating systems, networking fundamentals, networking security, TCP/IP networking, administration.

Timing & Duration of the training DAYS

OBJECTIVES

Describe Check Point Infinity's Consolidated Security Architec-

Explain the difference between the Harmony Endpoint On-Premises and Cloud management environ-

Identify the main components of the Harmony Endpoint Security Architec-

Identity the basic workflow for Harmony Endpoint Security Management.

Give examples of useful resources for Harmony Endpoint Security Manage-

Log in to the Web Management Console.

Navigate the Web Management interface to gain a basic understanding of the features and capabilities Harmony Endpoint provides for security management.

Discuss situations where it might be necessary to change default policy

Identify recommended releases for a Harmony Endpoint Client deploy-

Identify deployment prerequisites.

Given a deployment scenario, identify deployment methods, Endpoint Client packages, and the basic workflow.

Recognize the different types of data security available to deploy.

Describe how Full Disk Encryption protects and recovers data that is accessed and stored on Endpoint computers.

Identify how to secure removable media devices and protect ports.

Identify remote help and recovery capabilities.

Discuss the challenges of threat prevention.

Identify how Harmony Endpoint defends networks against advanced

Identify the key components in Harmony Endpoint simplified and large-scale deployments.

Identify sizing guidelines for Harmony Endpoint deployments.

Give examples of how to expand the solution with Super Nodes and External Policy Servers.

Identify the additional capabilities that High Availability (HA) and Active Directory configurations support.

Identify useful resources for basic troubleshooting.

Trening Centar Beograd

Give examples of potential problems or issues that might occur when using Harmony Endpoint.

Investigate and troubleshoot basic Harmony Endpoint troubleshooting scenarios.

Define Harmony Endpoint Management as a Service.

Explain the set-up process for Harmony Endpoint Management as a

Discuss the workflow when migrating from Endpoint On-Premises to Endpoint Management as a Service.

EXERCISES

Install the Endpoint Security Management Server

Deploy an Endpoint Security Management Server

Configure Endpoint for Deployment

Deploy Endpoint Security Clients to Hosts

Test and Analyze Threat Response

Configure LDAP Strong Authentication

Deploy a Secondary Endpoint Security Management Server

Troubleshoot Endpoint Communication Issues

Migrate from On-Premises to Endpoint Management as a Service

Connect Existing Hosts to Endpoint Management as a Service (Option-

Cybersecurity Boot Camp (CCSA & CCSE)

Course Overview

Technical professionals and experts who support, administer, or perform advanced deployment configurations of Check Point products. Learn basic and advanced concepts and develop skills necessary to administer IT security fundamental and intermediate tasks.

Prerequisites

One-year experience on Check Point products. Working knowledge of Windows, UNIX, networking technology, the Internet and TCP/IP is recommended.

SECURITY ADMINISTRATOR OBJECTIVES

Describe the primary components of a Check Point Three-Tier Architecture and explain how they work together in the Check Point environ-

Identify the basic workflow to install Security Management Server and Security Gateway for a single-domain

Create SmartConsole objects that correspond to the organization's topology for use in policies and rules.

Identify the tools available to manage Check Point licenses and contracts, including their purpose and use.

Identify features and capabilities that enhance the configuration and management of the Security Policy.

Demonstrate an understanding of Application Control & URL Filtering and Autonomous Threat Prevention capabilities and how to configure these solutions to meet an organization's security requirements.

Describe how to analyze and interpret VPN tunnel traffic. Identify how to monitor the health of supported Check Point hardware using the Gaia Portal and the com-

Describe the different methods for backing up Check Point system information and discuss best practices and recommendations for each method.

INGRAM MICRO | Trening Centar Beograd

Timing & Duration of the training DAYS

EXERCISES

Deploy SmartConsole

Install a Security Management Server

Install a Security Gateway

Configure Objects in SmartConsole

Establish Secure Internal

Manage Administrator Access

Manage Licenses

Create a Security Policy

Configure Order Layers

Configure a Shared Inline Layer

Configure NAT

Integrate Security with a Unified Policy

Elevate Security with Autonomous Threat Preven-

Configure a Locally Managed Site-to-Site VPN

Elevate Traffic View

Monitor System States

Maintain the Security Environment

SECURITY EXPERT OBJECTIVES

Identify the types of technologies that Check Point supports for automation.

Explain the purpose of the Check Management High Availability (HA) deployment.

Explain the basic concepts of Clustering and ClusterXL, including protocols, synchronization, and connection stickyness.

Explain the purpose of dynamic objects, updatable objects, and network feeds.

Describe the Identity Awareness components and configura-

Describe different Check Point Threat Prevention solutions.

Articulate how the Intrusion Prevention System is config-

Explain the purpose of Domain-based

Describe situations where externally managed certificate authentication is used.

Describe how client security can be provided by Remote Access.

Discuss the Mobile Access Software Blade.

Define performance tuning solutions and basic configuration workflow.

Identify supported upgrade methods and procedures for Security Gateways.

EXERCISES

Navigate the Environment and Use the Management API

Deploy Secondary Security Management Server

Configure a Dedicated Log Server Deploy SmartEvent

Configure a High Availability Security Gateway Cluster

Work with ClusterXL

Configure Dynamic and Updateable

Verify Accelerated Policy Installation and Monitoring Status

Elevate Security with HTTPS Inspection

Deploy Identity Awareness

Customize Threat Prevention

Configure a Site-to-Site VPN with an Interoperable Device

Deploy Remote Access VPN

Configure Mobile Access VPN

Monitor Policy Compliance

Report SmartEvent Statistics

Tune Security Gateway

Radware Alteon Level 1

Certification

- First try included as part of the course.
- Can be done from any location, only secure browser access required.

Comprised of two parts:

Hands-On Practical Exam

- Setup a given Alteon configuration, min score 75%
- Proctored by Radware, suggested to take the exam within the week of this class, latest two month after attending class.

Web-Based Certification Exam

- Multiple Choice Questions, min score 75%
- Take the web-based exam latest three month after practical exam.

If you pass both exams, you will be recognized as:
Radware Certified Alteon Specialist (RCAS-AL)

INGRAM MICRO® | Trening Centar Beograd

DAY 01

Alteon Course Agenda

Technical Overview Advanced Features

Setup Configuration

Using CLI and Web UI

Switching & Routing

Lab

High Availability

Lab

DAY 02

Server Load Balancing

Lab

Persistent SLB

Lab

SSL Services

Lab

Content Based SLB

Lab

Content Modification

Lab

Introduction to AppShape++

Lab

DAY 03

DAY 04

Vision Monitoring & Analytics & OTB

Lab

Troubleshooting

Lab

Hands-on Exam

Radware DefensePro level 1

Course Overview

This course covers DefensePro® product. Learn how to isolate, block and prevent application-level attacks, coupling unmatched security performance with advanced security intelligence. Understand how to securely connect and protect all mission-critical applications by thwarting viruses, intrusions, Trojans, worms and Denial of Service attacks. Learn how to eliminate security tool vulnerabilities and bottlenecks across all combined security architectures, overcoming the security vs. performance trade-off for fault-tolerant and highly scalable defense. The DefensePro Level 1 class is a structured 3-day course that is meant to highlight all the features and functions used on the DefensePro along with hands on labs to illustrate the protection mechanics

Objectives

Install and deploy a DefensePro based on deployments guidelines
Understand the different Attack Protection capabilities and how to configure them Navigate and use APSolute Vision Understand fundamentals of Vision Reporter

DAY 01

Introduction to DefensePro
Hardware Connectivity & Protection Policies
DefensePro Maintenance
Vision Analytics for DefensePro
Treasure Hunt Online Game

LAB

Initial configuration
Maintenance
Analytics

INGRAM MICRO | Trening Centar Beograd

DAY 02

BDoS Protection
DNS Protection
SYN Flood Protection
Out of State Protection
Basic Traffic Filters

LAB

BDoS
DNS
SYN
OOS
Traffic Filters

DAY 03

Signature Protection
Block/Allow Lists
Location based Mitigation & EAAF
Connection Limits
Basic Troubleshooting

LAB

Signature Protection
Block/Allow Lists
Connection Limits

CERTIFICATION

Comprised of two parts:

Hands-On Practical Exam

- Proctored by Radware, suggested to take the exam within one month of class.
- Web-Based Certification Exam
- Included as part of the course (First try)
- Can be done from any location

If you pass both exams, you will be recognized as: Radware Certified Security Specialist (RCSS)

Radware Alteon Secure (AppWall)

Course Overview

This course, Alteon Secure, is a structured 2-day certification training. It consists of a practical and a theoretical part. In this course we will focus on the features that extend the Alteon load balancer to an Application firewall. The course starts with all the basics needed to set up an Alteon Radware WAF from scratch and walks you through the various installation tasks. We explain how protection principles are set up and the basic concepts behind this solution. An introduction to the Radware WAF security filter is also included. For customers who own a DefensePro, we offer signaling to DefensePro to mitigate the attack at the perimeter. The configuration is covered in this training. We discuss monitoring with the local dashboard and Vision Analytics in theory and practice. Our final topic is troubleshooting. We explain the use of forensics to obtain information and how to fix the setup.

INGRAM MICRO® | Trening Centar Beograd

DAY 01

HTTP Basics
Web Application Security
Introduction to AppWall
Integrated AppWall Overview
AppWall Protection Principles
Lab Layout and Devices
Hands-On

DAY 02

AppWall Basic Cincepts
AppWall Filters Overview
AppWall Signaling to DefensePro
AppWall Monitoring and Reporting
AppWall Troubleshooting

Vmware vSphere: Install, Configure, Manage V8

Course Overview

This five-day course features intensive hands-on training that focuses on installing, configuring, and managing VMware vSphere 8, which includes VMware ESXi™ 8 and VMware vCenter® 8. This course prepares you to administer a vSphere infrastructure for an organization of any size. This course is the foundation for most VMware technologies in the software-defined data center.

DAY 01

Course Introduction

Introductions and course logistics

Course objectives

Explain basic virtualization concepts

vSphere and Virtualization Overview

Describe how vSphere fits in the software-defined data center and the cloud infrastructure

Recognize the user interfaces for accessing vSphere

Explain how vSphere interacts with CPUs, memory, networks, storage, and GPUs

DAY 02

Installing and Configuring ESXi

Install an ESXi host

Recognize ESXi user account best practices

Configure the ESXi host settings using the DCUI and VMware Host Client

Deploying and Configuring vCenter

Recognize ESXi hosts communication with vCenter

Deploy vCenter Server Appliance

Configure vCenter settings

Use the vSphere Client to add and manage license keys

Create and organize vCenter inventory objects

Recognize the rules for applying vCenter permissions View vCenter logs and events

DAY 03

Configuring vSphere Networking

Configure and view standard switch configurations

Configure and view distributed switch configurations

Recognize the difference between standard switches and distributed switches

Explain how to set networking policies on standard and distributed

Configuring vSphere Storage

Recognize vSphere storage technologies

Identify types of vSphere datastores

Describe Fibre Channel components and addressing

Describe iSCSI components and addressing

Configure iSCSI storage on ESXi

Create and manage VMFS datastores

Configure and manage NFS datastores

DAY 04

Deploying Virtual Machines

Create and provision VMs

Explain the importance of VMware Tools

Identify the files that make up a VM

Recognize the components of a VM Navigate the vSphere Client and examine VM settings and

Modify VMs by dynamically increasing resources

Create VM templates and deploy VMs from them

Clone VMs

Create customization specifications for guest operating systems

Create local, published, and subscribed content libraries

Deploy VMs from content libraries

Manage multiple versions of VM templates in content

vmware vSphere

Prerequisites

This course has the following prerequisites:

System administration experience on Microsoft Windows or Linux operating systems

Target Audience

System administrators

System engineers

DAY 04

Managing Virtual Machines

Recognize the types of VM migrations that you can perform within a vCenter instance and across vCenter instances

Migrate VMs using vSphere vMotion Describe the role of Enhanced vMotion Compatibility in migra-

Migrate VMs using vSphere Storage vMotion

Take a snapshot of a VM

Manage, consolidate, and delete snapshots

Describe CPU and memory concepts in relation to a virtualized environment

Describe how VMs compete for resources

Define CPU and memory shares, reservations, and limits

DAY 05

Deploying and Configuring vSphere Clusters

Create a vSphere cluster enabled for vSphere DRS and vSphere HA

View information about a vSphere cluster Explain how vSphere DRS determines VM placement on hosts in the cluster

Recognize use cases for vSphere DRS settings

Monitor a vSphere DRS cluster

Describe how vSphere HA responds to various types of failures

Identify options for configuring network redundancy in a vSphere HA

Recognize vSphere HA design considerations

Recognize the use cases for various vSphere HA settings

Configure a vSphere HA cluster

Recognize when to use vSphere Fault Tolerance

DAY 05

Managing the vSphere Lifecycle

Enable vSphere Lifecycle Manager in a vSphere cluster

Describe features of the vCenter Update Planner

Run vCenter upgrade prechecks and interoperability reports

Recognize features of VMware vSphere® Lifecycle ManagerTM

Distinguish between managing hosts using baselines and managing hosts using

Describe how to update hosts using baselines

Describe ESXi images

Validate ESXi host compliance against a cluster image and update ESXi hosts

Update ESXi hosts using vSphere Lifecycle Manager

Describe vSphere Lifecycle Manager automatic recommendations

Use vSphere Lifecycle Manager to upgrade VMware Tools and VM hardware

Veritas NetBackup 8.2: Administration

Course Overview

Veritas NetBackup 8.2: Administration is a five-day training that allows you to master data protection strategies. You will learn general principles, configuration and management With NetBackup, including how to best use NetBackup tools and interfaces, you monitor effectively backup operation and ensure that data recovery objectives are met.

Prerequisites

Attendees must be familiar with general network and storage concepts, administration and configuration of Windows or Linux operating systems.

INGRAM MICRO® | Trening Centar Beograd

DAY 01

Introducing NetBackup
Configuring NetBackup Storage
Configuring Policies

DAY 02

Performing File System Backups
Performing File System Restores

DAY 03

Configuring Disk Pools
Configuring Media Server Deduplication

DAY 04

Configuring and Managing Tape Storage Managing and Protecting the NetBackup Catalog

DAY 05

Optimizing File System Backups
Collecting Logs and Diagnostic Information

LAB OUTLINE:

This course includes hands-on lab exercises to apply your new skills in a virtual NetBackup domain. At the beginning of the class, students will choose between a NetBackup server with a Windows or Linux operating system, on which they will perform laboratory exercises.

NetBackup 8.2: Advanced Administration

Course Overview

Gain the skills for a successful data protection strategy with Veritas NetBackup 8.2. Advanced Administration Course. You will learn advanced NetBackup options, including performance enhancements
NetBackup, data loss recovery, application backups on physical and virtual machines, virtual machine accelerator backups and security. This course also covers usage
NetBackup for managing Oracle, Microsoft Exchange, Microsoft SQL, Microsoft SharePoint
backups and restores along with other modern workloads.

Prerequisites

Attendees should be familiar with general network and storage concepts, administration and configuration of Windows or Linux operating systems. Attendees must also have experience of one up to three years with basic NetBackup administration, configuration and operation. These prerequisites can be completed by attending any version of the NetBackup Administration course plus additional experience at work.

INGRAM MICRO® | Trening Centar Beograd

DAY 01

Improving NetBackup Performance
Securing the NetBackup Environment
Securing Backup Data
Auto Image Replication

DAY 02

Optimizing NetBackup Deduplication
Implementing NetBackup Cloud Solu-
Understanding Application Back-up Concepts
Managing Oracle Backups

DAY 03

Managing Microsoft SQL Backups
Managing Microsoft SharePoint Back-ups Managing Microsoft Exchange Backups Enhancing Virtual Machine

DAY 04

Disaster Recovery and NetBackup
Managing NDMP Backups
Modern workload protection
Managing NDMP Three-way backups

DAY 05

Managing Oracle backups using legacy policies
Managing Microsoft SQL backups using legacy policies
NetBackup API

LAB OUTLINE:

This course includes hands-on lab exercises to apply your new skills in a virtual NetBackup domain. At the beginning of the class, students will choose between a NetBackup server with a Windows or Linux operating system, on which they will perform laboratory exercises.

Veeam Backup & Replication v13

Configure, Manage, Recover

Course Overview

The Veeam® Backup & Replication v13training course is a four-day, technical deep dive focused on teaching IT professionals the skills to configure, manage and support a Veeam Availability Suite v12 solution. With extensive hands-on-labs, the class enables administrators and engineers to effectively manage data in an ever-changing technical and business environment, bringing tangible benefit to businesses in the digital world. This course is based on Veeam Availability Suite v12.

Prerequisites

Students should be experienced professionals with solid knowledge of servers, storage, networking

INGRAM MICRO® | Trening Centar Beograd

DAY 01

Introduction

Describe RTOs and RPOs, what they mean for your business, how to manage and monitor performance against them

The 3-2-1 Rule and its importance in formulating a successful backup strategy Identify key Veeam Availability Suite components and describe their usage scenarios and deployment types Building backup capabilities

Backup methods, the appropriate use cases and impact on underlying file systems

Create, modify, optimize and delete backup jobs, including Agents and NAS Backup jobs.

Explore different tools and methods to maximize environment perfor-

Ensure efficiency by being able to select appropriate transport modes while being aware of the impact of various backup functions on the infrastructure

DAY 02

Identify and describe the options available for replication and impacts of using them

Building replication capabilities

Create and modify replication jobs, outline considerations to ensure success Introduce the new Continuous Data Protection (CDP) policy

Secondary backups

Simple vs. advanced backup copy jobs, how to create and modify them using best practices to ensure

efficient recovery

Discuss using tapes for backups

Advanced repository capabilities

Ensure repository scalability using a capability such as SOBR on-premises and off-site including

integration with cloud storage

Ensure compatibility with existing deduplication appliances

Introduce the new hardened repository

DAY 03

Protecting data in the cloud

Review how Veeam can protect the data of a cloud native application

Review how Veeam Cloud Connect enables you to take advantage of cloud services built on Veeam

Review how Veeam can be used to protect your Office 365 data

Restoring from backup

Ensure you have the confidence to use the correct restore tool at the right time for restoring VMs, bare metal and individual content such as files and folders

Utilize Secure Restore to prevent the restoration of malware

Describe how to use Staged Restore to comply with things like General Data Protection Regulation

(GDPR) before releasing restores to production

Identify, describe and utilize the different explores and instant recovery tools and features

Cisco Umbrella Deployment and Configuration

Course Overview

The Cisco Umbrella Deployment and Configuration is a 1-day instructor-led course where you will learn to understand and position how Cisco Umbrella works and what are the features. Students who enter the course with a basic understanding of Cisco products and IT solutions will be able to describe the Cisco Umbrella, discuss Threat Intelligence, use Cisco Roaming Client

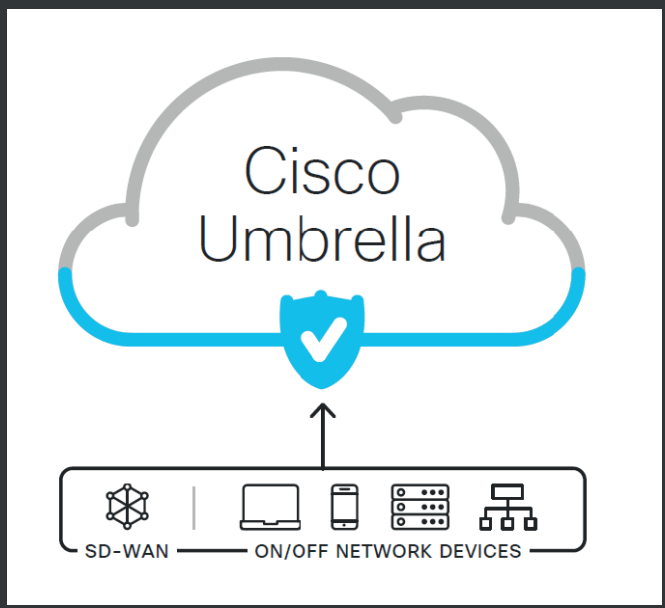
Prerequisites

Cisco recommends that you have the following knowledge and skills before taking this course: Familiarity with Ethernet, TCP/IP, and Security Internet-related networking

DAY 01

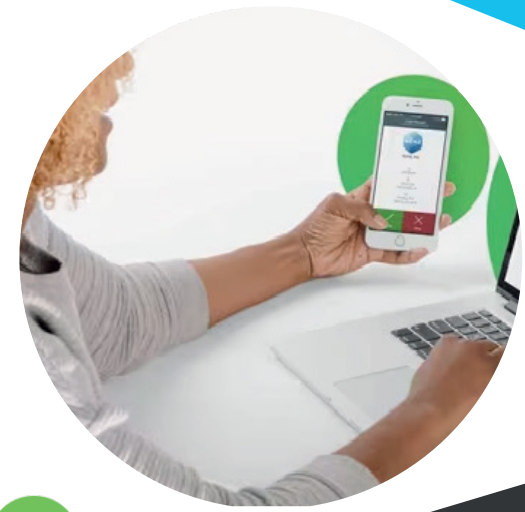
DNS Network Protection
Protecting whole organization in min-
utes Setting up basic policies
Active Directory User Sync
Making policies more granular
(per user/group)
About Umbrella VA
About Umbrella tunnels
Secure Remote Worker
Making protection work outside
of corporate network
Cloud Delivered Firewall
L7 firewall in the cloud
Secure Internet Gateway (Umbrella SIG)
Deployment options
Cloud-managed web-proxy
File inspection
HTTPS inspection
CASB controls
More granular controls over cloud apps
dCloud self-paced LAB

INGRAM MICRO® | Trening Centar Beograd



Cisco Secure Access by Duo Training

Course Overview



The Cisco Secure Access by Duo training is a 1-day instructor-led hands-on course which provides an introduction to Cisco Secure Access by Duo. Yo u will learn about Duo architecture, components, deployment, and integration with ASA/AnyConnect, ISE.

Prerequisites

Cisco recommends that you have the following knowledge and skills before taking this course:
Familiarity with Ethernet, TCP/IP, and Security
Internet-related networking

INGRAM MICRO® | Trening Centar Beograd

DAY 01

Overview

Architecture

Licensing

Deployment

Lab

Cisco Meraki Solutions

Course Overview

Cisco Meraki Solutions Training is a 1-day instructor-led hands-on course as an introduction to Meraki architecture and Meraki products where you will learn how to perform configuration related to Meraki Switch, Security appliance, Access points, Cameras and Sensors.

Prerequisites

It is recommended that you have the following knowledge and skills before taking this course:

Basic understanding of TCP/IP networking and network architecture

MERAKI 360

Meraki 360
Cloud-Managed Networks

DAY 01

INGRAM MICRO® | Trening Centar Beograd

Cisco Meraki cloud architecture, administration, and licensing, co-termination, and renewals

Basic hardware and features of all product families
Meraki Cloud Monitoring & Management for Catalyst

Security & SD-WAN:
Threat protection and content filtering rules
Design scalable Meraki Auto VPN architectures
Design dynamic path selection policies
Design stable, secure, and scalable routing deployments

Next-Gen Access:
Applying security at MS switches
Network access control solutions
Design Enterprise wireless services
MR wireless networks for Enterprise
MR wireless networks for guest access
Air Marshal

Network Assurance:
Wireless client connectivity issues using Dashboard

Smart Cameras and IoT:
Camera video and alerting
Retention settings

LAB OUTLINE:

MX introduction and practice with labs

MS introduction and practice with labs

MR introduction and practice with labs

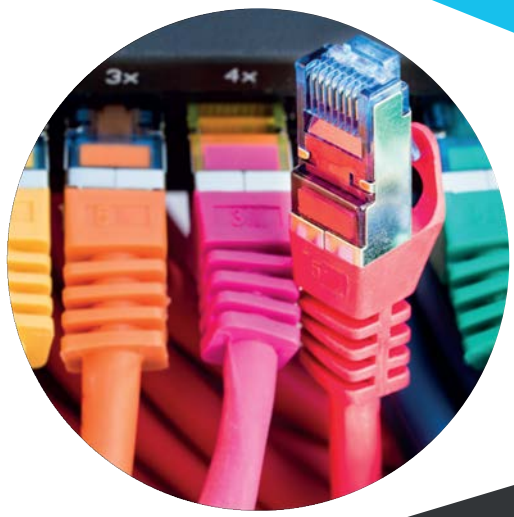
MV introduction and practice with labs

MT introduction and practice with labs

(ENARSI)

Cisco Enterprise Advanced Routing and Services

Course Overview



Cisco Enterprise Advanced Routing and Services is a 5-day instructor-led hands-on custom course
where you will learn about advanced routing and infrastructure technologies EIGRP Routing Protocol, OSPF Routing protocol , Routing Redistribution, BGP Architecture, MTU concept / Encapsulation, MPLS Architecture and MPLS L3VPNs.
All relevant topics are covered with corresponding labs in order to give hands-on experience to participants.

Prerequisites

It is recommended that you have the following knowledge and skills before taking this course: Good technical understanding of TCP/IP networking and network architecture

INGRAM MICRO | Trening Centar Beograd

DAY 01

Concept of IP Routing
EIGRP Introduction and Architecture
EIGRP Neighbor Formation
Route Exchange Composite Metric and Best
EIGRP Summarization and Filtering

DAY 02

OSPF Introduction and Architecture
OSPF Database and LSA Types
OSPF Inter Area and External Routes in the Data
OSPF Adjacenies Authentication and Network Type
OSPF Summarization and Filtering

DAY 03

Routing Protocol Redistribution
Policy-Based Routing (PBR)
VRF-Lite

DAY 04

BGP Introduction
BGP Peering ebgp and ibgp
BGP Route Reflectors
BGP Route Propogation Control
BGP Attributes and Best Path Selection Process
BGP Filtering Using ACL, Prefix Lists and Route Maps

DAY 05

MPLS Introduction
MTU concept / Encapsulation
MPLS Database and Control Plane
MPLS Building L3VPN Network
MPLS OSPF, BGP, EIGRP and Static Routing as a PE CE routing protocol in L3VPN

ENCOR

Implementing and Operating Cisco Enterprise Network Core Technologies

Course Overview

Implementing and Operating Cisco Enterprise Network Core Technologies is a 5-day instructor-led hands-on custom course where you will learn about advanced routing and infrastructure technologies EIGRP Routing Protocol, OSPF Routing protocol , Routing Redistribution, BGP Architecture and skills needed to configure, troubleshoot, and manage enterprise networks.

All relevant topics are covered with corresponding labs in order to give hands-on experience to participants.

DAY 01

- Layer 2 connectivity using VLANs and trunking
- Implementation of redundant switched networks using Spanning Tree Protocol
- Link aggregation using Etherchannel
- Configure and verify access control lists
- Implement Numbered and Named IPv4 ACLs
- Configure and explain Network Address Translation (NAT) on Cisco routers
- Configure Dynamic NAT and Port Address Translation (PAT)
- Configure Static NAT

INGRAM MICRO® | Trening Centar Beograd

DAY 02

- Concept of IP Routing, RIB, FIB and CEF
- OSPF Introduction and Architecture
- OSPF Database and LSA Types
- OSPF Inter Area and External Routes in the Data
- OSPF Adjacenies Authentication and Network Type
- OSPF Summarization and Filtering

ENCOR

Implementing and Operating Cisco Enterprise Network Core Technologies

Prerequisites

It is recommended that you have the following knowledge and skills before taking this course:

Good technical understanding of TCP/IP networking and network architecture

DAY 03

EIGRP Introduction and Architecture
EIGRP Neighbor Formation
Route Exchange Composite Metric and Best
EIGRP Summarization and Filtering
Routing Protocol Redistribution
Implementing Hot Standby Routing Protocol (HSRP)

INGRAM MICRO | Trening Centar Beograd

DAY 04

Policy-Based Routing (PBR)
VRF-Lite
Configuring Cisco IOS Embedded Event Manager (EEM)
Configure and Verify Cisco IP SLAs
Configure and Verify a Generic Routing Encapsulation (GRE) Tunnel
The purpose, function, features, and work-flow of Cisco DNA Center
The components and features of the Cisco SD-Access solution, including the nodes, fabric control plane, and data plane
The components and features of Cisco SD-WAN solutions, including the orchestration plane, management plane, control plane, and data plane

DAY 05

BGP Introduction
BGP Peering ebgp and ibgp
BGP Route Reflectors
BGP Route Propogation Control
BGP Attributes and Best Path Selection Process
BGP Filtering Using ACL, Prefix Lists and Route Maps

(CCNA)

Implementing and Administering Cisco Solutions

Course Overview

Cisco Implementing and Administering Cisco Solutions is a 5-day instructor-led hands-on custom course where course gives you a broad range of fundamental knowledge for all IT careers. Through a combination of lecture, hands-on labs, and self-study, you will learn how to install, operate, configure, and verify basic IPv4 and IPv6 networks. The course covers configuring network components such as Cisco switches and Cisco routers.

All relevant topics are covered with corresponding labs in order to give hands-on experience to participants.

Prerequisites

It is recommended that you have the following knowledge and skills before taking this course: Basic IP address knowledge, Basic computer literacy and Basic Internet usage skills

DAY 01

OSI model fast review

Explain the role and function of network compo-

Network topology architectures

Compare physical interface and cabling types

Interface and cable issues (collisions, errors, mismatch duplex, and/or

Compare TCP to UDP

Configure and verify IPv4 addressing and subnet-

Configure and verify IPv6 addressing and

Describe IPv6 address types

DAY 02

Features and functions of the Cisco Internetwork Operating System (IOS®) software

L2 Introduction

Switching Introduction and Switch Operation

VLANs and VTP

Introduction to Spanning Tree

Rapid and Rapid Per VLAN Spanning Tree

Rapid And Rapid Per VLAN Spanning Tree

Advance Spanning Tree Portfast, BPDU-

Ethernet Link Aggregation

Etherchannel Configuration

DAY 03

MTU concept: L2MTU / IP MTU difference

Concept of IP Routing

Features, metrics, and path selection concepts of routing protocols

Cisco IOS IP Routing: Operation, benefits, and limitations of static

Configuration of inter-VLAN routing

OSPF Introduction and

Open Shortest Path First (OSPF)v2 including adjacencies, packet types, and areas

DAY 04

DHCP Server Fundamentals

Configure and verify DHCP client and relay

Configure and verify access control lists

Implement Numbered and Named IPv4 ACLs

AAA - Management of Cisco devices / Implement a basic security configuration of the device management plane

Configure network devices for remote access using SSH

Configure and verify device access control using local passwords

Explain the function of SNMP in network operations

Syslog features including facilities and levels

DAY 05

Configure and explain Network Address Translation (NAT) on Cisco routers

Configure Dynamic NAT and Port Address Translation (PAT)

Configure Static NAT

Explain how Global Internet routing works

Implementing External Border Gateway Protocol (eBGP), path selection, and single and dual-homed networking

Implementing Internal Border Gateway Protocol (iBGP)

INGRAM MICRO® | Trening Centar Beograd

Cisco Secure Email Gateway Bootcamp

Course Overview

Cisco Secure Email Training is a 2-day instructor-led hands-on course where you will learn how to deploy Cisco Secure Email Gateway from scratch, as well as how the basic and advanced email security controls work to mitigate the security risk that comes from the email threat vector. With the exercises provided within a lab environment, you will be able to learn how to configure and verify the security controls configuration for inbound and outbound emails.

Prerequisites

Cisco recommends that you have the following knowledge and skills before taking this course: TCP/IP services, including Domain Name System (DNS), Secure Shell (SSH), FTP, Simple Network Management Protocol (SNMP), HTTP, and HTTPS Experience with IP routing

DAY 01

Overview

Licensing
Deployment
Platform options
Deployment Options
Initial Configuration
Email Pipeline and Email Security Manager
HAT and RAT
Antispam
Antivirus
AMP and MAR
Bounce Verification
Graymail Detection and Safe Unsubscribe
Content Filters
Outbreak Filters
Message Filters
URL Filtering
CUA
DLP
Secure Email GW LDAP integration
SMTP Authentication
Email (Sender) Authentication
Forged Email Detection
Email Encryption
DANE

INGRAM MICRO | Trening Centar Beograd

DAY 02

LAB:

Protecting Against Malicious or Undesirable URLs
Outbreak Filtering
Forged Email Detection
Macro Detection
Graymail Detection
Advanced Malware Protection (AMP)
DomainKeys Identified Mail (DKIM)
Sender Profile Framework (SPF)
Scenario - Domain-based Message Authentication, Reporting
Sender Domain Reputation (SDR)
Consuming External Threat Feeds (STIX/TAXII)
DNS-Based Authentication of Named Entities
Mailbox Auto Remediation for On-Prem Microsoft Exchange
Search & Remediate Email Via Message Tracking
Single Sign On using SAML 2.0
Support for Unified Common Event Format (CEF) based Logging
Ability to Safe Print Message Attachments
Improved Phishing Detection Efficacy with Cisco Cloud URL Analysis

Cisco Firepower Bootcamp

Course Overview

Next Generation Firewall Custom Training is a 2-day instructor-led hands-on course where you will learn how to secure your network with Cisco Firepower Threat Defense NGFW, using exercises in a lab environment. You will learn how to use and configure Threat Defense technology, including IPS, URL, AMP control, as well as how to take advantage of powerful tools to perform more effective event analysis, including detection of file types and malware based on your environment.

Prerequisites

Cisco recommends that you have the following knowledge and skills before taking this course:
Technical understanding of TCP/IP networking and network architecture
Basic familiarity with firewall and IPS concepts

INGRAM MICRO | Trening Centar Beograd

DAY 01

Introduction to NGFW

Platform Overview

FTD Management Options

FTD Deployment Modes

FTD Initial Config & FMC reg

FTD Security Zones

Access Control Policy

NAT on FTD

Flex Config

Prefilter

URL Filtering

Malware & File Policy

Intrusion Policy

LAB

DAY 02

Rate Limiting

VPNs

FTD Packet Flow

Resiliency Options

Multi-Instance mode

VRFs

Migration from ASA & others

New features overview

Licensing

LAB

Webex Calling Technical Bootcamp

Course Overview

The Cisco Webex Calling Configuration and Administration is a 3-day instructor-led hands-on course which provides an overview of the Cisco Webex Calling solution and Webex components.The main objective of this bootcamp is to enable participants to gain a solid understanding of Webex Calling Service, including its architecture, supported clients and devices, administration, licensing, features, provisioning, basic analytics, and troubleshooting and support. All relevant topics are covered with corresponding labs in order to give hands-on experience to participants. After completing this bootcamp, participants should be capable to identify and implement the right Webex Calling solution for simpler customer scenarios.

Prerequisites

Cisco recommends that you have the following knowledge and skills before taking this course: Technical understanding of TCP/IP networking and network architecture Participants should have basic understanding of telephony as well as fluent comprehension in spoken and written English

INGRAM MICRO® | Trening Centar Beograd

DAY 01

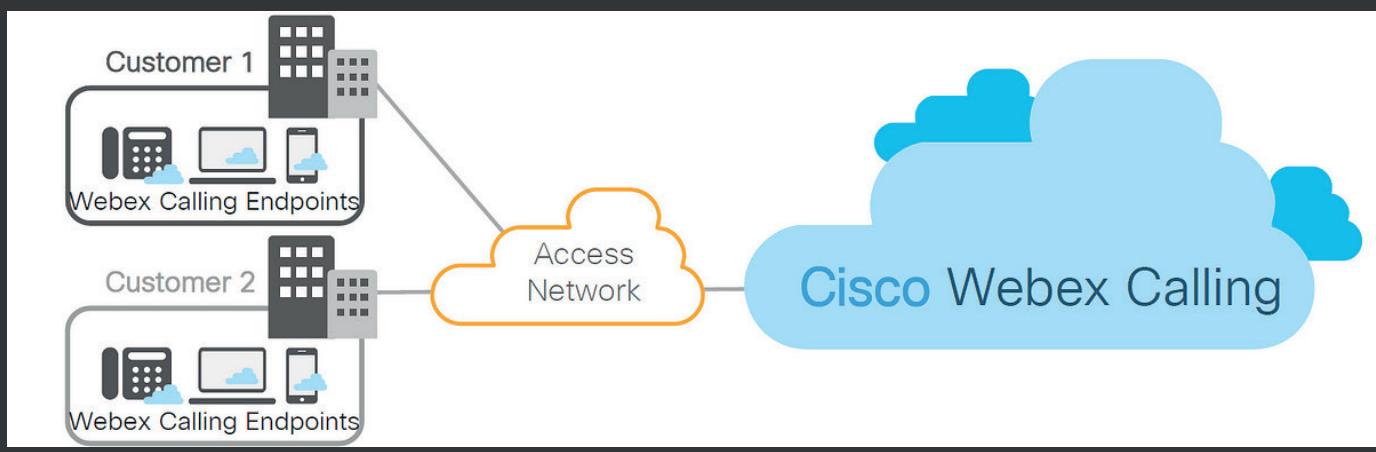
Product Overview
Architecture
Clients and devices
System Administration

DAY 02

Labs
Provisioning
Local Gateway
Location features

DAY 03

User Features
Analytics and Troubleshooting
Support
Customer Scenarios



Cisco/Viptela SD-WAN Bootcamp

Course Overview

The Cisco SD- WAN Deplo yment, Configur ation and Administr ation is a 3-day instructor -le d hands-on course which pr ovides an o ver vie w of the Cisco SD- WAN solution and SD- WAN comp onents . Cisco SD- WAN is a new te chnolog y, this aining co vers salient featur es such as zer o-touch provisioning, se cure netw ork bring-up , configur ation using featur e templates , configur ation of Ov erlay Manag ement Pr oto col (OMP) and p olicies for netw ork traffic manag ement. Y ou will learn ho w to manag e, and op er ate a se cure extensible netw ork using Cisco SD- WAN o ducts , best pr actices for configuring r outing pr oto cols in the data center and the br anch, as w ell as how to implement advance d contr ol, data, and application-awar e p olicies . The course also co vers SD- WAN deplo yment and migr ation options , placement of contr ollers , how to deplo y WAN Edg e de vices .

Prerequisites

Cisco recommends that you have the following knowledge and skills before taking this course: Technical understanding of TCP/IP networking and network architecture Basic familiarity with firewall Strong understanding of routing protocol operation, including both interior and exterior

INGRAM MICRO® | Trening Centar Beograd

DAY 01

Cisco SD-WAN Architecture

Cisco SD-WAN Terminology and Key Functions

Controller Deployment Options: Design considerations and constraints

Data Plane Bring-up: ZTP, Bootstrapping, Manual Provisioning

DAY 02

Configuration Templates: Device and Feature templates

OMP and Service Side Routing

Designing and Implementing Control Policies

DAY 03

Designing and Implementing Data Policies

Designing and Implementing Application-Aware

SD-WAN Security (Ent. FW, URL Filtering)

Licensing

LAB OUTLINE:

Manage and Monitor SD-WAN Components

Deploy and Verify SD-WAN vEdge Routers

Deploy SD-WAN Templates

SD-WAN Overlay Routing

SD-WAN Policies

Cisco ISE Fundamentals Training

Duration: 1 day

Objective: Provide understaning of Cisco ISE and teaches you to deploy, configure, and operate Cisco ISE as the central platform for identity-based access control and its basic services.

INGRAM MICRO | Trening Centar Beograd

Agenda:

1 day

- Introducing Cisco ISE Network Security Architectures and the Main Functions
- Introducing Cisco ISE Deployment; Cisco ISE node personas, supported deployment models, licensing considerations.
- Introduction to User roles and profiles, Identity Sources and Authentication Types (MAB and 802.1X in Cisco ISE)
- Network Device Integration with Cisco ISE
- Guest Access and Guest Portals Overview
- Introducing Cisco ISE Policy Configuration
- Exploring System administrators and accounts, Global Logging and Reporting

Wi-Fi Fundamentals Training

Course overview

Wi-Fi Fundamentals is a 1-day training that provides a comprehensive foundation in wireless networking, beginning with core RF principles such as radio wave propagation, signal measurement, and link budget analysis. It then explores essential 802.11 technologies, including standards, regulatory domains, channel usage, and radio resource management.
Participants will gain a clear understanding of antenna behavior, MIMO, and beamforming, and how these impact real-world Wi-Fi performance. The course concludes with key infrastructure considerations, covering PoE, cabling, and switching requirements for effective wireless deployments.

Pre-requisites

This course is a foundational training, so deep prior experience in RF or wireless is not required. However, familiarity with the topics below will help participants to better grasp the concepts:

- awareness of cabling types and basic transmission concepts
- general knowledge of network devices (switches, routers and access points)
- basic network knowledge (understanding of IP network addressing, subnetting, basic switching concepts).

Agenda

Duration: 1 day

- RF Fundamentals
- Propagation of radio waves
- RF Signal measurement
- Signal Strength
- Interference, Noise, Rogue AP
- Device Capabilities
- SNR
- Principles of RF mathematics
- dB, dBm, dBi calculations
- Link budget analysis
- Power calculations
- Wi-Fi antenna characteristics
- Antenna patterns and gain
- Polarization and diversity
- Beamforming and MIMO
- Technology Fundamentals
- Wi-Fi Governance
- Regional Regulatory Bodies
- IEEE 802.11 Standards
- Wi-Fi Alliance
- BUsable Channels and Power Combinations
- BRegional EIRP limitation examples
- Frequency Bands
- RRM Fundamentals
- Fundamentals
- Infrastructure Considerations
- Physical Infrastructure Connections
- PoE standards and requirements
- Cable infrastructure and backbone
- Switch port configurations

Introduction to Basic AI concepts and IBM AI Tools and Models

INGRAM MICRO | Trening Centar Beograd

Course Overview

This training provides an introduction to fundamental AI concepts and IBM AI tools and models. Participants will explore various AI applications, including machine learning, natural language processing, digital assistants and RAG. Various use-cases will demonstrate how to use different AI tools to build and deploy AI powered solutions. Additionally, attendees will learn about IBM's AI platforms and services, such as watsonx, watsonx Assistant etc. The workshop aims to enhance practical knowledge in AI and familiarize participants with IBM's AI ecosystem.

Audience

AI beginners, sellers, and technical professionals interested in learning about AI concepts and IBM AI tools.

Labs included: **No**

Duration: 1 day

What you will learn

- ☑ Fundamental AI concepts and applications
- ☑ Techniques for data preparation and model training
- ☑ Methods for evaluating AI models
- ☑ How to use AI to improve business processes
- ☑ Exploring IBM's AI platforms and services

IBM watsonx.ai Technical Sales Workshop (L3 labs)

INGRAM MICRO | Trening Centar Beograd

Course Overview

This workshop covers the IBM watsonx.ai L3 badge lab, highlighting some of the core components and capabilities of IBM watsonx-.ai with additional L3+ labs that can be included based on client interest.

Audience

Technical sellers and engineers interested in learning about AI concepts and IBM AI tools

Labs included: Yes

Duration: 1 day

What you will learn

- The watsonx.ai web based Prompt Lab UI, including Structured and Freeform interface, sample prompts, model information panels and model parameter panel.
- Strengths and weaknesses of different models
- An overview of the model parameters and how they influence output.
- Zero shot vs. Few shot prompting
- Using prompts to generate specific output
- Saving prompts and prompt sessions
- Restoring a prompt to an earlier state via prompt history
- Saving prompts to a Jupyter notebook and working with the Jupyter notebook

Agenda

- Navigation and zero shot prompting
- Parameter config and output formats
- One-shot prompts, saving prompts
- Using Notebooks
- Langchain integration
- RAG using Watson Discovery
- RAG using VectorDB
- Integrating Assistant with watsonx Foundation Models

IBM watsonx.ai Technical Workshop (L4 Labs)

Course Overview

This workshop consists of labs focused on implementing and integrating generative AI use cases using watsonx.ai. Participants will explore various applications of LLMs, including generation, summarization, and classification. Hands-on exercises will demonstrate how to integrate LLMs with client applications. Labs will cover the LangChain framework and Retrieval Augmented Generation (RAG). Additionally, attendees will learn about prompt engineering, prompt tuning, and generating synthetic data with new foundation models. The workshop aims to enhance practical skills in AI and LLM integration.

INGRAM MICRO | Trening Centar Beograd

Audience

Engineers interested in learning about AI concepts and IBM AI tools

Labs included: Yes

Duration: 1 day

What you will learn

- ☑ How to implement generative AI use cases using watsonx.ai.
- ☑ Techniques for integrating LLMs with client applications.
- ☑ Utilizing Python code samples and Streamlit for LLM applications.
- ☑ Applying the LangChain framework for LLM applications.
- ☑ Implementing the Retrieval Augmented Generation (RAG) pattern with LLMs.
- ☑ Using Elasticsearch as a vector database for RAG.
- ☑ Exploring prompt engineering and prompt tuning techniques.
- ☑ Performing prompt tuning using the Tuning Studio on IBM watsonx.ai.
- ☑ Generating synthetic data for AI model testing and tuning.
- ☑ Discovering new foundation models available in watsonx.ai.

Agenda

- ☑ Introduction to Generative AI in watsonx.ai
- ☑ Large language model application building blocks
- ☑ LangChain
- ☑ Implement RAG Use Cases
- ☑ RAG on documents with LangChain and Elasticsearch
- ☑ Prompt Tuning
- ☑ Generate synthetic data

IBM watsonx.data Technical Sales Workshop

INGRAM MICRO | Trening Centar Beograd

Course Overview

This workshop covers the IBM watsonx.data L3 badge lab, highlighting some of the core components and capabilities of IBM watsonx.data. This workshop also covers additional labs that can help integrate different products.

The watsonx.data component (the focus of this workshop) makes it possible for enterprises to scale analytics and AI with a data store built on an open lakehouse architecture, supported by querying, governance, and open data and table formats, to access and share data.

Audience

Technical sellers and engineers interested in learning about IBM data lakehouse tools.

Labs included: Yes

Duration: 1 day

What you will learn

- The watsonx.data web-based user interface (UI), including infrastructure management, data management, running SQL statements, and managing user access
- The Presto web interface and the Presto command line interface (CLI)
- MinIO object storage
- Ingesting data into watsonx.data
- Creating schemas and tables
- Running queries that combine data from multiple data sources (data federation)
- Offloading tables from Db2 into watsonx.data
- Rolling back a table to a previous point in time

Agenda

- Exploring the watsonx.data User Interface
- Working with Presto
- Working with MinIO
- Data Ingest
- Federated Queries
- Offloading Data from a Data Warehouse
- Time Travel and Rollback

INTRODUCTION TO JUNIPER WORLD & JUNOS

Summary: Introduction to Juniper world of networking with focus on Junos-based device management.

Duration: 2 days

Objective: To get you ready for JNCIA-Junos exam!

Labs included: Yes.

Audience: Junior networking/infrastructure engineers and administrators.

What you will learn:

- Concepts, benefits, and functionality of the Junos OS core elements

- Concepts, operation, and functionality of the Junos user interfaces
- The main elements for configuring Junos devices
- Configuring basic components of a Junos device
- Methods for monitoring and maintaining Junos devices
- Basic routing concepts and functionality for Junos devices
- Configuring and monitoring basic routing elements for a Junos device
- Concepts and functionality of routing policy and firewall filters on Junos devices

Agenda:

Day 1:

- Juniper Portfolio
- Networking Fundamentals
- Junos OS Fundamentals
- User Interfaces
- Configuration Basics
- Operational Monitoring and Maintenance
- Labs

Day 2:

- Routing Fundamentals
- Routing Policy
- Firewall Filters
- Labs

Junos®

Juniper Networks | Engineering Simplicity

INGRAM MICRO TRAINING CENTER

INTRODUCTION TO JUNIPER MIST AI

Juniper Mist™

Summary: This introductory Juniper Mist Cloud training course is designed for network engineers and architects who use the Mist Cloud to build, manage, and maintain their wireless, wired, and WAN networks from anywhere—with a focus on wireless networks. It involves basic introductions to Mist features such as: Mist APIs, Marvis, location-based services, cloud services, and monitoring and analyzing the Mist Cloud platform.

Duration: 1 day

Objective: Learn basics about Juniper MIST AI and prepare for JNCIA-MISTAI exam.

Labs included: Yes, and live instructor-led demo.

Audience: Networking engineers and administrators.

What you will learn:

Juniper Mist™

- Describe Mist AI and the Mist Cloud
- Describe the Mist AI Cloud features and devices
- Connect to the Mist Cloud
- Create and manage accounts in the Mist Cloud
- Manage and configure the Mist Cloud general settings
- Manage and configure the Mist Cloud secondary settings
- Manage Mist access points
- Describe Wireless Assurance
- Describe Wired Assurance
- Use Mist monitoring and analytics tools
- Use Mist Marvis AI Assistant
- Describe Mist location-based services and use cases
- Use the Mist API
- Explain the help options
- Live Demo

JUNIPER NETWORKS | Engineering Simplicity

INGRAM MICRO TRAINING CENTER

JUNIPER AI-DRIVEN ENTERPRISE (AIDE)

Juniper Mist™

Summary: The Juniper Mist AI Platform makes networking predictable, reliable and measurable with unprecedented visibility into the user experience. Time-consuming manual IT tasks are replaced with AI-driven proactive automation and self-healing capabilities, lowering networking operational costs and saving substantial time and money.
Juniper's AI-Driven Enterprise portfolio enables customers to scale and simplify the deployment of their campus wired and wireless networks while bringing greater insight and automation to network operators. An enhancement to the Juniper Mist Cloud and AI engine, EVPN-VXLAN campus fabric management is part of Wired Assurance, and it expands on Juniper's unique automation, AIOps, and cloud capabilities to streamline IT operations, lower IT costs, and deliver unparalleled agility and scale.

Duration: 1 day

Objective: Understand the features and benefits of Juniper AIDE.

Labs included: Yes, and live instructor-led demo.

Audience: Networking engineers and administrators.

What you will learn:

- Fundamentals of AI-driven Enterprise
- AI-driven Enterprise Portfolio
- Mist AI and the Mist Cloud
- Marvis Virtual Network Assistant
- Wireless Assurance
- Mist Edge – WAN forwarding
- Location Services
- Wired Assurance
- Device Provisioning
- Switch Templates
- Campus Fabric Architectures
  - EVPN Multihoming
  - Campus Fabric Core-Distribution
  - Campus Fabric IP Clos
- WAN Assurance
- Juniper WAN Design
- Data Center Assurance

Juniper Mist™

JUNIPER NETWORKS | Engineering Simplicity

INGRAM MICRO TRAINING CENTER

JUNIPER INTENT-BASED DATA CENTER FUNDAMENTALS

Summary: TThis course provides introductory instruction on data center switching using Juniper products. This course lays the foundational knowledge necessary to understand a data center that is built upon an IP fabric, as well as Ethernet VPN – Virtual Extensible LAN (EVPN-VXLAN) architecture. Attendees will be given a background on modern data center design and intent-based networking concepts.

Duration: 1 day

Objective: Understand the architecture of modern data center networking fabrics and learn the basics about Apstra, a multi-vendor intent-based data center management platform

Audience: Networking/infrastructure engineers and administrators.

What you will learn:

Juniper Apstra™

- Juniper DC Portfolio
- Challenges of Traditional Data Centers
- Data Center Architectures (VCF, IP Fabrics)
- Designing Data Center
  - Leaf-Spine Architectures
  - Designing Oversubscription
  - Design Considerations and Guidelines
  - QFX Roles and Positioning in a Datacenter
- IP Fabrics Basics
  - Data Center Routing and Switching
  - IP Fabrics Underlay
  - VXLAN Functions and Operation Overview
  - EVPN Functions and Operation Overview
- Apstra Introduction – Intent Based Networking
- Apstra Capabilities
- Apstra Components
- Apstra Reference Designs
- Apstra Day 0/Day 1/Day 2 Assurance

JUNIPER NETWORKS | Engineering Simplicity

INGRAM MICRO TRAINING CENTER

SECURING YOUR JUNIPER NETWORKS

JUNOS

Juniper Connected Security

Summary: This course provides you with the foundational knowledge required to work with the Junos operating system and to configure Junos security devices. The course provides a brief overview of the Juniper security products and discusses the key architectural components of the Junos software. Key topics include UI options with a heavy focus on CLI, configuration tasks typically associated with the initial setup of devices, interface configuration basics with configuration examples, secondary system configuration, and the basics of operational monitoring and maintenance of Junos Security devices. The course then delves into foundational knowledge of security objects, security policies, and configuration examples including types of security objects, security policies, security services NAT, site-to-site IPsec VPN, and Juniper Secure Connect VPN. Through demonstrations and hands-on labs, students will gain experience in configuring and monitoring Junos OS and monitoring basic device operations on the SRX Series device.

Duration: 2 days

Objective: To get you ready for JNCIA-Sec exam!

Labs included: Yes

Audience: Junior networking/infrastructure engineers and administrators.

Juniper Connected Security

What you will learn:

- Juniper Security Products
- Juniper Architectural Components
- Interface Configuration Basics
- Security Object and Policies Configuration
- NAT Concepts and Configuration
- IPsec VPN Concepts and Configuration
- Juniper Security Technologies (IPS, Integrated User-Based Firewall, ATP)
- Virtual SRX
- SRX Troubleshooting and Monitoring

Junos®

Day 1:

- Introduction to Juniper Security
- Juniper Connected Security Overview
- Juniper SRX Overview and Initial Configuration
- Security Zones and Screen Objects
- Address Objects and Service Objects
- Security Policies
- Labs

Day 2:

- Source (NAT) Network Address Translation (Lab)
- Destination NAT (Lab)
- Static NAT (Lab)
- IPsec VPN Concepts
- Site-to-Site IPsec VPN (Lab)
- Juniper Security Technologies
- Integrated User-Based Firewall
- IPS
- Juniper ATP Cloud
- Juniper Unified Threat Management (UTM)
- Virtual SRX

ADVANCED BGP FOR SERVICE PROVIDERS

Summary: This two-day course is designed to provide attendees with detailed coverage of BGP and routing policy on products using Junos OS. Through examples, demonstrations, and hands-on labs, attendees will gain experience in protocol operations, configuring, monitoring, and troubleshooting BGP on Junos devices.

Duration: 2 days

Objective: Detailed coverage of BGP and routing policy in Juniper Junos OS

Labs included: Yes.

Audience: Individuals responsible for implementing, monitoring and troubleshooting BGP in a service provider's network.

What you will learn:

- BGP operations implementation in Juniper Junos OS
- The route selection process for BGP and how to alter it in Juniper Junos OS
- BGP attributes and how these attributes can be used to manipulate traffic
- How policies function in Juniper Junos OS
- Manipulate BGP attributes using routing policy
- Route reflector concepts, operation and configuration in Juniper Junos OS
- Configure advanced options for BGP peers
- Configure BGP multipath in Juniper Junos OS
- Identify route flap and the causes for route instability
- Route damping concepts, operation and configuration in Juniper Junos OS
- BGP and route policy monitoring and troubleshooting

Agenda:

Day 1:

- Module 1
  - BGP Operations
  - BGP Session Establishment Configuration Options
- Module 2
  - BGP Path Selection
  - BGP Attributes and Policy, Part 1
- Module 3
  - BGP Attributes and Policy, Part 2

Day 2:

- Module 4
  - BGP Scalability, Route Reflectors
- Module 5
  - Advanced BGP Peering Options
  - BGP Multipath
  - BGP Route Damping
- Module 6
  - BGP Monitoring and Troubleshooting

INTRODUCTION TO JUNOS OS – ONE-DAY ESSENTIALS

Summary: This training provides a practical introduction to Juniper Networks and Junos OS for network engineers who are new to the Junos operating system. The course focuses on Junos fundamentals, device architecture, basic configuration, and operational workflows, enabling participants to confidently perform initial device setup and day-to-day operations.

Duration: 1 day

Objective: By the end of this training, participants will understand Junos OS architecture and core design principles, navigate and configure devices using the Junos CLI , implement essential system, interface, and routing settings, apply routing policies and firewall filters, use key network utilities, and perform operational monitoring, troubleshooting, and basic system management on Junos devices.

Labs included: Yes

Audience: Network engineers and administrators with general networking knowledge who are working with Junos OS for the first time. The course level is Beginner-to-Intermediate.

What you will learn:

Junos OS architecture and processes: control vs. forwarding plane, software structure, key system components

Junos CLI proficiency: navigation, command syntax, context-sensitive help, operational vs. configuration modes, show/edit/commit workflows

Initial device configuration: management access, hostname, users and authentication, time/NTP, basic system services, and rescue configuration

Core configuration concepts: configuration hierarchy, candidate vs. active config, commit/rollback, load/merge/replace, and compare

System & interfaces: interface families and units, descriptions, addressing, and validation using operational commands

Routing fundamentals: routing and forwarding tables, route preference, next-hop resolution, static routes, OSPF/BGP essentials, ECMP/load-balancing behavior and verification

Routing policy & firewall filters: match/then logic, policy application points, common use-cases, stateless filter structure, counters, and placement

Network utilities: ping, traceroute, monitor traffic / packet capture basics, and interface/route verification commands

Operations & maintenance: system health checks, monitoring workflows, software/log management, and first-line troubleshooting

Agenda

Module 1: Junos OS Fundamentals

Module 2: Junos User Interface and Core Configuration Concepts

Module 3: Routing Fundamentals

Module 4: Routing Policy and Firewall Filters

Module 5: Network Utilities

Module 6: Network Management

Module 7: Operations, Monitoring and Maintenance

Lab: Juniper Day One + Experience

IMPLEMENTING DATA CENTER FABRIC WITH EVPN AND VXLAN

Duration: 5 days

Summary: This five-day course provides in-depth instructions on IP fabric and Ethernet VPN–Virtual Extensible LAN (EVPN-VXLAN) data center design and configuration. The course covers other data center concepts, including basic and advanced data center design options that include collapsed spine and super spine architectures, Data Center Interconnect (DCI), EVPN multicast enhancements, and seamless EVPN-VXLAN stitching. Through demonstrations and hands-on labs, students will gain experience with these features.

Objective: Provide detailed coverage of IP fabric and Ethernet VPN–Virtual Extensible LAN (EVPN-VXLAN) data center design and configuration

Labs included: Yes

Audience: Individuals responsible for designing and implementing data centar using Juniper products.

What you will learn:

- Basic and advanced data center design concepts
- How to configure an IP fabric
- How to configure an EVPN-VXLAN data center
- How to configure enhanced loop protection
- How to configure centrally routed bridging (CRB) EVPN-VXLAN
- How to configure edge-routed bridging (ERB) EVPN-VXLAN
- How to configure symmetric EVPN Type 2 routing
- How to configure Data Center Interconnect (DCI)
- How to configure seamless EVPN-VXLAN stitching
- How to configure filter-based forwarding
- Enhancements to multicast functionality in an EVPN-VXLAN

IMPLEMENTING DATA CENTER FABRIC WITH EVPN AND VXLAN

Day 1

Modern Architectures
- Traditional multitier architecture challenges
- Next-generation data center architectures

IP Fabric Underlay Routing
- What an IP fabric is
- Routing in an IP fabric

IP Fabric Underlay Scaling
- How to properly scale an IP fabric

IP Fabric Underlay Configuration
- How to configure an OSPF-based IP fabric underlay network
- How to configure an EBGP-based IP fabric underlay network

Lab 1: IP Fabric

VXLAN Overview
- Layer 2 connectivity over a Layer 3 network
- VXLAN Fundamentals

VXLAN Gateways
- Purpose and function of VXLAN gateways

EVPN Overview
- EVPN functionality
- EVPN control in a VXLAN deployment

Day 2

EVPN Protocol
- Describe EVPN routing and bridging

Configuring EVPN-VXLAN Networks
- Discuss how to configure EVPN-controlled VXLAN

Lab 2: Configuring EVPN-VXLAN Networks

Enhanced Ethernet Segment Loop Protection
- Describe the loop potential
- Describe and configure the ES loop-detect protocol

Basic Data Center Architectures
- Describe basic architectures and deployment scenarios

Basic Data Center Architectures
- Describe basic architectures and deployment scenarios

Super Spine Configuration
- Describe a super spine architecture
- Configure a super spine

Day 3

Configuring Centrally Routed Bridging
- Describe EVPN-VXLAN reference architectures
- Describe centrally routed and bridging
- Configure centrally routed and bridging

Lab 3: Configure Centrally Routed Bridging
Configuring Edge-Routed Bridging
- Describe edge-routed bridging
- Explain how to configure edge-routed bridging
- Explain how to verify edge-routed bridging operations

Lab 4: Configuring Edge-Routed Bridging
MAC-VRF Overview
- Describe the benefits of deploying MAC-VRFs
- Identify data center architectures for MAC-VRF use
- Describe the MAC-VRF design options

MAC-VRF Configuration
- Describe the requirements of deploying MAC-VRFs
- Describe the MAC-VRF use case
- Configure common parameters
- Configure a VLAN-based MAC-VRF
- Configure a VLAN-aware MAC-VRF
- Configure a VLAN-bundle MAC-VRF

Lab 5: MAC-VRF Configuration
Symmetric Routing Using Type 2 EVPN
- Describe asymmetric routing
- Describe symmetric routing
- Implement symmetric routing

Lab 6: Symmetric Routing Configuration

Day 4

DCI with EVPN–VXLAN Network
- Discuss DCI with EVPN-VXLAN Network

Configuring DCI
- Discuss how to configure DCI in the data center

Lab 7: Data Center Interconnect
Seamless EVPN-VXLAN Stitching
- Explain the purpose of seamless EVPN-VXLAN stitching
- Discuss seamless EVPN-VXLAN design options
- Describe a packet walkthrough for seamless EVPNVXLAN stitching

Configuring Seamless EVPN-VXLAN Stitching
- Explain how to configure seamless EVPN-VXLAN stitching
- Describe how to verify EVPN-VXLAN stitching operations

Lab 8: Implementing Seamless EVPN-VXLAN Stitching

Day 5

Filter-Based Forwarding
- Discuss the purpose of filter-based forwarding in a data center
- Explain how to configure filter-based forwarding in a data center
- Describe how to verify filter-based forwarding in a data center

Lab 9: Implementing Filter-Based Forwarding

EVPN Multicast Extensions
- Describe the multicast extensions to EVPN

EVPN Multicast Configuration
- Explain how to configure EVPN multicast

EVPN Multicast Assisted Replication
- Describe the potential problem with EVPN multicast
- Illustrate a use case
- Describe assisted replication
- Configure assisted replication
- Describe assisted replication with SMET

JUNOS ENTERPRISE SWITCHING – ONE-DAY ESSENTIALS

Summary: This one day training provides a practical introduction to Enterprise Layer 2 switching on Junos OS. The course focuses on essential Ethernet switching concepts and configuration examples using Junos Enhanced Layer 2 Software. It includes an overview and demonstrations of key switching operations and high availability (HA) features, enabling participants to develop the skills and confidence to configure, verify, monitor, and troubleshoot enterprise Layer 2 switching environments.

Duration
1 days

Objective: By the end of this training, participants will understand Junos Layer 2 switching architecture; configure and verify core switching functions; implement VLANs, IRBs, multiple Spanning Tree Protocol (STP) options, LAGs, and RTGs; deploy Virtual Chassis and high availability features such as GRES, NSR, and NSB to improve network resilience; and use operational tools to monitor and troubleshoot enterprise switching networks.

Labs included: Yes.

Course Level: Intermediate

Audience: Network engineers and administrators with general networking knowledge who want to expand their skills in Juniper Enterprise Layer 2 switching. This course is suitable for professionals responsible for configuring, operating, or supporting Junosbased switching platforms in enterprise environments.

Prerequisites:

- Basic understanding of networking concepts (Ethernet, VLANs, Layer 2 switching)
- Familiarity with Junos OS fundamentals and basic experience with the Junos CLI (operational and configuration modes).

What you will learn

- Module 1: Ethernet Switching and Layer 2 Operations and Design
- Module 2: Basic Enterprise Switching Implementation
- Module 3: Implementing VLANs and IRBs
- Module 4: Spanning Tree Protocols Options and Protection Features
- Module 5: Storm Control
- Module 6: LAGs and RTGs
- Module 7: Deploying Virtual Chassis
- Module 8: Deploying High Availability: GRES, NSR, and NSB
- Module 9: IP Telephony Features: PoE, LLDP, Voice-VLAN
- Module 10: Layer 2 Security Features Overview
- Module 11: Monitoring and Troubleshooting Layer 2 Enterprise Networks
- Labs