Business Ecosystems

Training Centre

Business Ecosystems

Training Programmes

Enterprise Network

Enterprise Security

Service Provider

May 2018

Content

Enterprise Network

Associate

Basic Course in Network Technologies

p. 3

Switching

Course in Switching in Local Networks

p. 4

Routing

Course in Internal Routing in IP Networks

p. 3

LNS

Linux OS Network Services Course

p. 8

IPv6

IPv6 Implementation Course

p. 4

Design

Course in Computer Network Design

p. 9

Enterprise Security

Associate

Basic Course in Network Technologies

p. 3

Switching

Course in Switching in Local Networks

p. 4

VPN

Virtual Private Networks Course

p. 5

ASA

Course in Firewalls and SSL VPN

p. 6

AAA

Course in Access Administration in Computer Networks

p. 8

LSS

Linux Security Services Course

p. 9

Service Provider

Associate

Basic Course in Network Technologies

p. 3

Routing

Course in Internal Routing in IP Networks

p. 3

BGP

Course in Internet Routing in IP Networks

p. 5

MPLS

Basic Course in MPLS Services

p. 6

AMPLS

Advanced Course in MPLS Services

p. 7

IOS XR

Carrier-Class Training Course

p. 7

Associate

Basic Course in Network Technologies

Course Description

The course is intended for:

- engineers responsible for building and maintaining of small networks;
- first-line technical support specialists.

Course Objective

To obtain the knowledge and skills necessary to configure and operate small networks (10–20 network devices) and to troubleshoot.

At the end of the course

You will:

- know the principles of data transmission networks;
- have an understanding of network protocols and services in accordance with the OSI model;
- have knowledge of Cisco network devices architecture;
- have the skills of hardware diagnostics of Cisco network devices operation;
- use the command line for configuring switches and routers, as well as tools for building a network topology;
- understand the principles of the operation of access control lists (ACL) and be able to apply them;
- be able to configure basic network services on Cisco equipment (DNS, DHCP, NTP);
- be able to configure static and dynamic routing;
- be able to configure Internet access technologies such as NAT, Reflexive-ACL, IP Inspect;
- have an understanding of WAN and VPN networks;
- be able to troubleshoot small networks.

Course Summary

Module	Subject	Duration
1	Theory of building local networks and architecture of Cisco network devices	8 ac. hrs
2	Configuring switching technologies	8 ac. hrs
3	Remote access methods and packet filtering	8 ac. hrs
4	Routing in data networks	8 ac. hrs
5	Organization of Internet access	8 ac. hrs

Recommended Preliminary Training

Basic computer literacy, OS Windows or Linux working skills. General idea of methods of building communication networks. Experience in working with IP-networks is preferable.

Routing

Course in Internal Routing in IP Networks

Course Description

The course is intended for:

- engineers responsible for development and maintaining of networks using dynamic routing protocols.

Course Objective

To obtain the knowledge and skills necessary for the implementation and operation of dynamic routing protocols in an enterprise network.

At the end of the course

You will:

- understand the principles of NMBA-networks using the example of Frame-Relay technology;
- have knowledge of Cisco network devices architecture;
- implement dynamic routing Cisco EIGRP protocol in an enterprise network;
- implement the dynamic routing OSPF protocol in several areas;
- configure dynamic routing to connect to an operator using the BGP protocol;
- create policies for routing records exchange between routing protocols;
- troubleshoot the operation of dynamic routing protocols.

Course Summary

Module	Subject	Duration
1	Frame-Relay overview	4 ac. hrs
2	Cisco routers architecture	4 ac. hrs
3	Configuring the EIGRP Routing Protocol	8 ac. hrs
4	Using the OSPF routing protocol at the enterprise	8 ac. hrs
5	Basic setting of the BGP Internet routing protocol and policies application	16 ac. hrs

Recommended Preliminary Training

“Associate” training or alternative training.

Switching

Course in Switching in Local Networks

Course Description

The course is intended for:

- Specialists responsible for building and maintaining networks using Cisco Catalyst switches.

Course Objective

To obtain the knowledge and skills necessary to configure and operate switching technologies in local networks, and to troubleshoot.

At the end of the course

You will:

- know the principles of building switched networks;
- understand and be able to implement VLAN, Q-in-Q, Etherchannel, UDLD, DTP and VTP technologies;
- configure RPVST + and MST loop prevention protocols with advanced STP Toolkit functions;
- implement the protocols of the fault-tolerant HSRP, VRRP and GLBP gateway;
- understand and apply methods for managing traffic processing order: CBWFQ, WRED, Policing and Shaping, L2 QoS;
- understand and be able to configure security technologies for a switched environment: Port-Security, Storm-Control, VACL, Private VLAN, DHCP Snooping, 802.1x.

Course Summary

Module	Subject	Duration
1	Principles of building a switched network	8 ac. hrs
2	Loop prevention protocols	6 ac. hrs
3	Gateway fault-tolerance protocols	4 ac. hrs
4	Configuring L2 and L3 QoS technologies	12 ac. hrs
5	Switched networks security	10 ac. hrs

Recommended Preliminary Training

“Associate” training or alternative training.

IPv6

IPv6 Implementation Course

Course Description

The course is intended for:

- information systems administrators;
- engineers responsible for building and maintaining IPv6 networks using network equipment.

Course Objective

Obtain the knowledge and skills necessary for the implementation and operation of IPv6 protocol based networks.

At the end of the course

You will:

- know how IPv6 works;
- understand address classification in IPv6;
- use IPv6 in access control lists;
- понимать работу DHCPv6;
- understand the operation of DHCPv6;
- have an understanding of the principles of multicasting in IPv6;
- be able to implement dynamic routing protocols for IPv6: RIPng, EIGRPv6, OSPFv3, MP-BGP, IS-IS;
- manage routing records between dynamic routing protocols;
- use IPv4 <-> IPv6 tunnels;
- use address translation mechanisms.

Course Summary

Module	Subject	Duration
1	Basics of IPv6	2 ac. hrs
2	IPv6 dynamic routing protocols	8 ac. hrs
3	Tunneling between IPv4 and IPv6	2 ac. hrs
4	How IPv6 protocol multicast works	2 ac. hrs
5	Converting addresses between IPv4 and IPv6	2 ac. hrs

Recommended Preliminary Training

“Associate”, “Routing” training or alternative training.

VPN

Virtual Private Networks Course

Course Description

The course is intended for technical specialists who design, implement and maintain virtual private networks built on the basis of IPSec technology.

Virtual Private Network (VPN) is an important tool for building corporate data networks with the ability to encrypt the transmitted traffic.

The Cisco IOS toolkit provides a whole range of technologies suitable for different scenarios.

Course Objective

To obtain the knowledge and skills necessary to configure and operate VPN technologies in an enterprise network.

At the end of the course

You will:

- know the principles of IPSec technology;
- have an understanding of the public key infrastructure (PKI);
- configure network-to-network tunnels: IPSec, IPSec VTI, GRE, GRE over IPSec, DMVPN, GET VPN;
- implement remote access technologies using PPTP, L2TP, Easy VPN, DVTI, SSL;
- troubleshoot VPN networks.

Course Summary

Module	Subject	Duration
1	The architecture of IPSec	8 ac. hrs
2	Public Keys Infrastructure	6 ac. hrs
3	Configuring the VPN network-to-network	14 ac. hrs
4	Configuring VPN for remote access	8 ac. hrs
5	Troubleshooting VPN	4 ac. hrs

Recommended Preliminary Training

“Associate”, “Routing”, “Switching” training or alternative training.

BGP

Course in Internet Routing in IP Networks

Course Description

The course is intended for:

- information system administrators;
- engineers of service operators and large enterprises, responsible for building and maintaining networks using the BGP dynamic routing protocol.

Course Objective

To obtain the knowledge and skills necessary to install and operate the BGP dynamic routing protocol in the networks of service providers and enterprises; and to troubleshoot.

At the end of the course

You will:

- know the principles of the BGP protocol;
- understand the scenarios for applying path attributes: AS-PATH, Local Preference, MED, WEIGHT, etc.;
- configure filters for routing records;
- apply methods for updating routing policies: soft-reconfig, route-refresh, and ORF;
- use the COMMUNITY attribute to logically separate routing records;
- implement scalable BGP protocol scenarios using peer-group, peer-template, routereflector, confederation;
- understand the role of the BGP protocol for the operation of MPLS VPN and IPv6 technologies;
- troubleshoot BGP networks.

Course Summary

Module	Subject	Duration
1	Basics of working in ASA OS	2 ac. hrs
2	Configuring filtering and translation technologies	8 ac. hrs
3	Routing and switching by means of firewalls	4 ac. hrs
4	Implementation of VPN technologies	8 ac. hrs
5	Using instruments of increasing availability and scalability	2 ac. hrs

Recommended Preliminary Training

“Associate”, “Routing” training or alternative training.

ASA

Course in Firewalls and SSL VPN

Course Description

The course is intended for information security specialists, responsible for segmentation, network shielding and the creation of flexible VPN access to enterprise resources.

Course Objective

Obtain the knowledge and skills necessary to build secure networks using Cisco ASA equipment.

At the end of the course

You will:

- understand the principles of Cisco ASA firewalls;
- segment networks using firewalls;
- implement routing and switching protocols on Cisco ASA firewalls;
- understand the scenarios for the use of firewalls;
- configure VPN network-to-network technologies;
- configure flexible and manageable VPN remote access, using SSL VPN;
- implement firewalls in fault-tolerant mode;
- use virtualization technology with security contexts;
- troubleshoot.

Course Summary

Module	Subject	Duration
1	Basics of working in ASA OS	4 ac. hrs
2	Configuring filtering and translation technologies	8 ac. hrs
3	Routing and switching by means of firewalls	4 ac. hrs
4	Implementation of VPN technologies	8 ac. hrs
5	Using instruments of increasing availability and scalability	8 ac. hrs

Recommended Preliminary Training

“Associate”, “Routing”, “Switching”, “VPN” training or alternative training.

MPLS

Basic Course in MPLS Services

Course Description

The course is intended for engineers responsible for implementing network services using multiprotocol MPLS switching in enterprise networks and service providers.

Course Objective

To obtain the knowledge and skills necessary to install and operate network services in enterprise networks and service providers.

At the end of the course

You will:

- understand the principles of MPLS technology and Cisco routers architecture;
- select MPLS services for the implementation of the tasks;
- implement MPLS technology and MPLS L3 VPN service;
- implement internal and external routing protocols at the PE-CE edge;
- set up equipment to support PIM Multicast: Dense Mode, Sparse Mode, SSM, MSDP;
- implement the MPLS Multicast VPN service;
- troubleshoot MPLS networks.

Course Summary

Module	Subject	Duration
1	The architecture of MPLS services	4 ac. hrs
2	Configuring MPLS as a service platform	8 ac. hrs
3	Introduction of L3 MPLS VPN technology	4 ac. hrs
4	Configuring Multicast support equipment	6 ac. hrs
5	Introduction of MPLS Multicast VPN	2 ac. hrs

Recommended Preliminary Training

“Associate”, “Routing”, “BGP” training or alternative training.

AMPLS

Advanced Course in MPLS Services

Course Description

The course is intended for engineers responsible for implementing network services using multiprotocol MPLS in the networks of service providers.

Course Objective

To obtain the knowledge and skills necessary to install and operate network services in the networks of service providers.

At the end of the course

You will:

- apply Carrier Supporting Carrier technology to support providers;
- implement MPLS L3 VPN in the Inter-AS scenario using the A/B/C options;
- implement Inter-AS Multicast MPLS VPN;
- implement L2 VPN technologies: AToM, L2TPv3, VPLS;
- manage network traffic using MTPL Traffic Engineering technology;
- understand protection against distributed DOS-attacks;
- troubleshoot MPLS networks.

Course Summary

Module	Subject	Duration
1	Application of CSC technology	4 ac. hrs
2	Building Inter-AS MPLS L3 VPN	8 ac. hrs
3	Building Inter-AS MPLS Multicast VPN	4 ac. hrs
4	Implementation of L2 VPN technologies	8 ac. hrs
5	Application of MPLS Traffic Engineering	8 ac. hrs

Recommended Preliminary Training

“Associate”, “Routing”, “BGP”, “MPLS” training or alternative training.

IOS XR

Carrier-Class Training Course

Course Description

The course is intended for network engineers responsible for building and maintaining networks using high-performance Cisco ASR/XR/GSR/CRS series equipment running on the Cisco IOS-XR operating system.

Course Objective

To obtain the knowledge and skills necessary to install and operate the equipment based on the Cisco IOS-XR in the networks of service providers; and to troubleshoot.

At the end of the course

You will:

- describe the architecture of Cisco IOS-XR based network devices;
- implement RIP, EIGRP, OSPF, IS-IS, BGP routing protocols;
- configure MPLS and Traffic Engineering technologies;
- implement MPLS L2VPN and MPLS L3VPN in Intra-AS and Inter-AS scenarios;
- configure equipment to support multicasting;
- troubleshoot Cisco-OS-XR.

Course Summary

Module	Subject	Duration
1	Basics of working in Cisco IOS-XR	8 ac. hrs
2	Configuring routing protocols	8 ac. hrs
3	Introduction of MPLS, MPLS TE and MPLS VPN technologies	8 ac. hrs
4	Configuring Multicast support equipment	4 ac. hrs
5	Service migration from Cisco IOS to Cisco IOS-XR	4 ac. hrs

Recommended Preliminary Training

“Associate”, “Routing”, “BGP”, “MPLS”, “AMPLS” training or alternative training.

LNS

Linux OS Network Services Course

Course Description

The course is intended for engineers responsible for implementing network services using Linux.

Course Objective

To obtain the knowledge and skills necessary to install and operate network services in Linux based enterprise networks.

At the end of the course

You will:

- be able to configure NTPD, DNSD, DHCPD, FTPD, SCPD, NFS, RSYNC, SQUID, WCCP, VMPS network services;
- configure the Linux router as a router-on-a-stick supporting 802.1Q tags;
- implement RIP, OSPF, BGP dynamic routing protocols;
- implement NAT, CARP, VRRP technologies;
- monitor networks using SYSLOG, SNMP, TFTP, NetFlow, SPAN, RMON;
- understand the interaction of Linux networks with Microsoft Windows networks (LDAP integration);
- Perform basic configuration of Apache, NGINX, SENDMAIL/POSTFIX, MySQL, Postgress application servers.

Course Summary

Module	Subject	Duration
1	Configuring network services	8 ac. hrs
2	Using Linux as a router	8 ac. hrs
3	Network monitoring	8 ac. hrs
4	Configuring application servers	4 ac. hrs
5	Interacting with Microsoft Windows Networks	4 ac. hrs

Recommended Preliminary Training

“Associate”, “Routing”, “Switching” training or alternative training.

AAA

Course in Access Administration in Computer Networks

Course Description

The course is intended for network engineers and information security specialists responsible for building networks with centralized management. The course covers the work of the AAA on Cisco Linux in conjunction with the BE ACS server.

Course Objective

Obtain the knowledge and skills necessary to install and operate Cisco IOS-XR based equipment in the networks of service providers; and to troubleshoot.

At the end of the course

You will:

- describe the architecture of the RADIUS protocol;
- describe the architecture of the TACACS + protocol;
- configure AAA on Linux and Cisco clients;
- implement the AAA BE-ACS server;
- troubleshoot AAA operations.

Course Summary

Module	Subject	Duration
1	RADIUS architecture	4 ac. hrs
2	TACACS+ architecture	3 ac. hrs
3	Configuring AAA on Cisco and Linux clients	3 ac. hrs
4	Configuring the AAA server	4 ac. hrs
5	Troubleshooting	2 ac. hrs

Recommended Preliminary Training

“Associate”, “Switching”, “VPN”, “ASA”, “LNS” training or alternative training.

LSS

Linux Security Services Course

Course Description

The course is intended for information security specialists responsible for the implementation of security services using Linux.

Course Objective

To obtain the knowledge and skills necessary to install and operate network services in the networks of service providers.

At the end of the course

You will:

- apply packet filter and iptables;
- implement VPN technologies based on OpenVPN, Remote Access (SSH, SSL, PPTP, GRE, etc.);
- use Squid proxy server to organize WebVPN;
- evaluate security of systems and services using Nmap and Nessus scanners;
- evaluate security of confidential information transmitted over the network using an Ethercap scanner;
- configure the RADIUS/TACACS protocol client;
- configure the clients of 802.1x protocol.

Course Summary

Module	Subject	Duration
1	Configuring iptables	4 ac. hrs
2	Building VPN networks	8 ac. hrs
3	Configuring WebVPN	4 ac. hrs
4	Assessing security of systems and services	8 ac. hrs
5	Using RADIUS/TACACS/802.1x protocols	8 ac. hrs

Recommended Preliminary Training

“Associate”, “VPN”, “LNS”, “AAA” training or alternative training.

Design

Course in Computer Network Design

Course Description

The course is intended for design engineers, personnel of corporate systems development services responsible for designing multi-service networks using Cisco equipment.

Course Objective

To obtain the knowledge and skills necessary to design multi-service networks.

At the end of the course

You will:

- describe the basic principles of designing wired and wireless networks;
- describe the basic principles of designing routing protocols;
- describe the basic principles of designing security services;
- describe the basic principles of data centre network design;
- describe the basic principles of designing service provider networks.

Course Summary

Module	Subject	Duration
1	Designing wired and wireless networks	8 ac. hrs
2	Designing routing protocols	8 ac. hrs
3	Designing security services	8 ac. hrs
4	Designing data centre networks	8 ac. hrs
5	Designing service provider networks	8 ac. hrs

Recommended Preliminary Training

Enterprise Network, Enterprise Security, Service Provider training or alternative training.

Business Ecosystems

Business Ecosystems, LLC.

143026 Moscow, Russia
Territory of Skolkovo Innovation Centre
1 Malevich St., office 5

E-mail: info@becsys.ru
Web-site: www.becsys.ru