BLACKBIRD FOR TRAINING

Master Networking: Advanced Security & Admin Certification Course



Master Networking: Advanced Security & Admin Certification Course

Network administration and security certification denotes the structured operational oversight, traffic telemetry analysis, and defensive policy enforcement across multi-tier enterprise telecommunications infrastructure. Master Networking: Advanced Security & Admin Certification is a one-week practitioner course for systems administrators and infrastructure engineers who require an Enterprise Administration and Security Playbook. Delegates evaluate traffic profiles, implement switching controls, configure perimeter filters, and maintain regulatory telemetry audit baselines.

Introduction

Enterprise telecommunications environments require systematic administration and multi-tier defensive controls to protect mission-critical workload delivery. This practitioner course aligns with the ISO/IEC 27033 telecommunications security standard, the NIST SP 800-41 guidelines on firewalls and firewall policy, and the IETF RFC 8446 transport security standard. Delegates explore operational protocols through an inspection walkthrough and hands-on simulation mode, testing switching hierarchies, packet routing logic, stateful packet filtering, and cryptographic transport layers against realistic operational disruption scenarios.

Course Objectives

- Define foundational switching topologies and administrative boundaries across multi-tier campus environments.
- Distinguish between stateful inspection firewalls and stateless access control lists to eliminate filtering latency.
- Compare interior gateway protocols against exterior routing protocols when provisioning high-availability failover paths.
- Select appropriate cryptographic tunnelling suites to secure telemetry transmission across untrusted intermediate networks.
- Apply quality-of-service queue disciplines to prioritise latency-sensitive operational traffic during packet contention.
- Justify network segmentation boundaries using zero-trust zoning models to minimise blast radius risks.



Target Audience

- Enterprise systems administrators managing campus switches and routing engines who must decide traffic scheduling configurations.
- Network operations engineers operating perimeter security filters who must choose between packet filtering methods.
- Infrastructure support specialists overseeing corporate telecommunications links who must evaluate path redundancy protocols.
- Information security administrators monitoring intrusion detection sensors who must determine traffic anomaly containment actions.
- Technical compliance officers reviewing network audit trails who must establish log retention parameters.

Course Outline

Day 1: Architectural Foundations and Campus Administration

- Core vs Distribution Switching: Designing High-Availability Campus Backbones and Redundant Links
- Spanning Tree Protocol: Eliminating Layer Two Forwarding Loops Across Enterprise LANs
- VLAN Trunking Protocol: Propagating Domain Information Across Multi-Switch Switching Hierarchies
- Link Aggregation Control Protocol: Bundling Physical Interfaces for Resilient Bandwidth Capacity
- Administrative Boundary Isolation: Enforcing Role-Based Operational Access Controls on Network Gear

Day 2: Traffic Pattern Analysis and Capacity Planning

- Flow Telemetry vs Packet Capture: Analysing Enterprise Bandwidth Consumption Metrics
- Quality of Service Queuing: Managing Latency and Jitter for Mission-Critical Corporate Traffic
- Predictive Modelling Methods: Forecasting Telecommunications Bandwidth Expansion and Hardware Demands
- Dynamic Routing Protocols: Establishing Fast Convergence Using Open Shortest Path First
- Bottleneck Identification Routines: Resolving Intermediate Node Contention Within Core Networks

Day 3: Data Centre Switching and Virtual Fabric Topologies

- Spine-and-Leaf vs Three-Tier Architecture: Optimising East-West Virtual Machine Data Centre Flows
- Virtual Local Area Networks: Segmenting Tenant Workloads Across Physical Switching Hardware
- Software-Defined Networking Fabrics: Centralising Overlay Orchestration and Programmable Control Planes
- Virtual Routing and Forwarding: Isolating Overlapping Administrative IP Subnets on Shared Switches
- Storage Area Network Switching: Prioritising Block-Level Storage Payloads Across Converged Networks



Day 4: Wide Area Networking and Transport Hardening

- Multiprotocol Label Switching vs SD-WAN: Provisioning Resilient Distributed Branch Telecommunications
- Border Gateway Protocol: Directing Autonomous System Routing Paths for Enterprise Multi-Homing
- Internet Protocol Security: Constructing Encrypted Virtual Private Gateways for Remote Sites
- Transport Layer Security: Protecting Administrative Web Interfaces and Node Telemetry Streams
- Traffic Policing and Shaping: Enforcing Committed Information Rates Across Leased Telecommunications Circuits

Day 5: Administrative Security Implementation and Playbook Finalisation

- Stateless Access Lists vs Stateful Firewalls: Enforcing Perimeter Packet Filtering Across DMZ Segments
- Network Address Translation Rules: Conserving Public Addresses and Concealing Internal Network Addresses
- Telemetry Audit Logging: Retaining Centralised Syslog Records for Compliance Verification Workflows
- Incident Response Containment Drills: Mitigating Rogue Network Devices and Spoofed DHCP Servers
- Final Playbook Production: Completing the Enterprise Administration and Security Playbook for Operations

Skills You Will Gain

- Campus switching topology configuration
- Flow telemetry performance analysis
- Spine-and-leaf fabric routing
- Software-defined overlay administration
- Cryptographic tunnel provisioning
- Stateful perimeter firewall filtering
- Zero-trust micro-segmentation enforcement
- Network capacity forecasting

Why Attend This Course

- From managing uncoordinated local switch configurations to directing unified multi-tier campus switching topologies.
- From relying on reactive network fault detection to interpreting predictive traffic flow telemetry and capacity forecasts.
- From operating basic perimeter boundary filters to deploying stateful inspection rules and zero-trust segmentation zones.
- From handling undocumented administration changes to completing an authoritative Enterprise Administration and Security Playbook.



Conclusion

Network administration and security certification develops rigorous technical control over physical switching layers, transport routing engines, and defensive boundaries. The course distinguishes between stateless filtering and stateful inspection, three-tier layouts and spine-and-leaf virtualised fabrics, and private line routing and software-defined wide area architectures. This one-week course is appropriate for enterprise administrators and infrastructure engineers tasked with maintaining reliable, resilient, and fully documented telecommunications platforms across modern business environments.

Course FAQs

What is network administration and security certification?

Network administration and security certification represents the formal demonstration of technical competency in managing, optimising, and securing enterprise telecommunications equipment, dynamic routing protocols, switching fabrics, and boundary filtering tools across multi-tier corporate environments.

What is the difference between stateful inspection and stateless packet filtering?

Stateless filtering evaluates each packet in isolation against static rule parameters, whereas stateful inspection tracks the connection state of active network conversations, verifying context, sequence numbers, and protocol validity before granting transit through perimeter firewalls.

Which standards does this networking course follow?

This course follows the ISO/IEC 27033 telecommunications security standard, the NIST SP 800-41 guidelines for firewall rule management, and IETF RFC 8446 transport security specifications to ensure standards-aligned infrastructure design and administration practices.

Is this course right for systems administrators?

Yes, systems administrators responsible for managing enterprise switching, wide area connections, perimeter security gateways, and operational traffic telemetry gain direct practical tools to build resilient and auditable network infrastructure.

What will delegates produce during the course?

Delegates produce an Enterprise Administration and Security Playbook containing validated campus switching profiles, traffic QoS queues, virtual fabric configurations, perimeter firewall rulesets, and incident containment procedures ready for operational deployment.

