Huawei ICT Competition 2022-2023 Exam Outline

Network Track

1. Overview

1.1. Network Track of Huawei ICT Competition Preliminary Stage Overview

Competition Stage	Exam Type	Duration	Number of Questions	Question Types	Total Score
Preliminary Stage	Written	90 Minutes	60	True/False Question, Single-Choice Question and Multiple-Choice Question	1000

1.2. Network Track of Huawei ICT Competition National Stage Overview

Competition Stage	Exam Type	Duration	Number of Questions	Question Type	Total Score
National Stage	Written	90 Minutes	90	True/False question, single-choice question and multiple-choice question	1000

Note: From the date of successful registration to the end date of the national, 10 bonus points will be acquired for passing any of HCIA-Datacom/Security/WLAN certifications, 30 bonus points for any of HCIP-Datacom/Security/WLAN certifications, and 50 bonus points for any of HCIE-Datacom/Security/WLAN certifications. These bonus points can be combined up to a maximum of 100 points.

1.3. Network Track of Huawei ICT Competition Regional Stage Overview

Competition Stage	Exam Type	Duration	Number of Questions	Question Type	Number of Contestants	Total Score
Regional Stage	Written	60 Minutes	60	True/False question, single-choice question and multiple-choice question	3(Personnel)	1000

	Lab	4 Hours	/	/	3 (as a team)	1000

Remark: The final score=30% * the average score of the written exam of 3 examinees in the same team + 70% * the score of the lab exam of the team.

1.4. Network Track of Huawei ICT Competition Global Stage Overview

Competition Stage	Exam Type	Duration	Number of Contestants	Question Type	Total Score
Global Stage	Lab	8 Hours	3 (as a team)	Comprehensive lab	1000

2. Weighting

2.1. Network Track of Huawei ICT Competition Preliminary Stage Weighting

Competition Stage	Direction	Weight
Preliminary Stage	Datacom	50%
	Security	30%
	WLAN	20%

2.2. Network Track of Huawei ICT Competition National Stage Weighting

Competition Stage	Direction	Weight
National Stage	Datacom	50%
	Security	30%
	WLAN	20%

2.3. Network Track of Huawei ICT Competition Regional Stage Weighting

Competition Stage	Direction	Weight
Regional Stage	Datacom	50%
	Security	35%
	WLAN	15%

2.4. Network Track of Huawei ICT Competition Global Stage Weighting

Competition Stage	Direction	Weight
Global Stage	Datacom	50%
	Security	40%
	WLAN	10%

3. Scope

3.1. Overview of Exam Contents

The Network Track exam contents cover knowledge about datacom, security, and WLAN technologies, including but not limited to routing protocols, Layer 2 switching technologies, IPv6 technologies, Huawei firewall features, VPN technologies, and WLAN networking and configurations.

3.2. Knowledge to Be Tested

Datacom

1. Datacom basics and TCP/IP protocol basics
2. Fundamentals, applications, and configurations of STP, RSTP, and MSTP switching
3. Fundamentals and applications of Ethernet technologies, VLAN, Eth-Trunk, stacking, and clustering
4. Fundamentals and applications of IPv6 basics, stateless autoconfiguration, and DHCPv6 and IPv6 transition technologies
5. Fundamentals and applications of static routing, OSPF, OSPFv3, IS-IS (IPv4), IS-IS (IPv6), BGP, BGP4+, and routing policies
6. WAN protocols (such as PPP) and PPPoE, as well as the applications of these protocols on Huawei routers
7. Fundamentals and configurations of MPLS, MPLS VPN, GRE VPN, L2TP, and IPsec VPN
8. Fundamentals and configurations of routing control technologies: ACL, IP prefix list, routing policy, etc.
9. Fundamentals and configurations of network reliability technologies: VRRP, BFD, etc.
10. Fundamentals and configurations of network services: Telnet, FTP, DHCP, etc.
11. Implementation of network management, such as the fundamentals and configurations of SNMP
12. SDN fundamentals and networking: VXLAN, BGP EVPN, iMaster NCE applications, etc.
13. Fundamentals and configurations of multicast: IGMP, PIM, etc.
14. Fundamentals and configurations of QoS

15. Segment Routing fundamentals: SR-MPLS, SRv6, etc.
16. Fundamentals and configurations of programming automation, and implementation of network automation, such as fundamentals and applications of SSH, NETCONF, YANG, Telemetry, OPS, and RESTful

Security

1. Security information and security overview: information security standards and specifications, privacy protection, common information security threats, threat defense, and information security development trends
2. Network security basics: common network devices, basic network protocols, firewall security policies, NAT, and firewall hot standby
3. Security attack and defense technologies: host security and hardening, web security, data security, network intrusion and defense, anti-DDoS, packet filtering, blacklist and whitelist, content filtering, and antivirus
4. Encryption and decryption technologies: encryption and decryption algorithms, PKI certificate system, and application of cryptographic technologies
5. VPN technologies: L2TP VPN, GRE VPN, IPsec VPN, SSL VPN, L2TP over IPsec, etc.
6. Advanced firewall features and networking: intelligent uplink selection, SLB, bandwidth management, virtual system, IPv6 technology, typical security networking design, etc
7. Security operations and analysis: security O&M operations, log management, security audit, and dynamic awareness technologies
8. Endpoint security technologies: user management, endpoint security system deployment, endpoint security system O&M, user authentication technologies, wireless network security technologies, etc

WLAN

1. WLAN technology fundamentals: WLAN standard organizations, WLAN frequency bands, 802.11 protocols, and WLAN antenna technologies
2. WLAN networking models: Fat AP, WAC + Fit AP, cloud AP, hot standby backup, dual-link backup, N+1 backup, and Mesh
3. WLAN implementation and deployment: CAPWAP fundamentals, AP onboarding, STA onboarding, and WLAN configuration
4. WLAN roaming: common roaming, fast roaming using PMK caching, 802.11r roaming, smart roaming, etc.
5. Radio resource management: radio calibration, load balancing, WLAN anti-interference technology, QoS, and VIP experience assurance
6. WLAN topologies, 802.11 protocols, 802.11 PHY technologies, and CAPWAP fundamentals
7. WLAN security and defense: device management, user access security policies, intrusion detection, antivirus, attack detection and defense, port isolation, CAPWAP tunnel encryption, etc.
8. WLAN access control technologies: 802.1X authentication, Portal authentication, MAC address authentication, hybrid authentication, and authentication and authorization
9. WLAN and IoT convergence and WLAN positioning technologies
10. WLAN IPv6 network and IPv6 fundamentals
11. CloudCampus solution, VXLAN, underlay, fabric, and overlay
12. WLAN O&M: traditional O&M and intelligent O&M based on CampusInsight
13. WLAN network planning and design

14. WLAN fault troubleshooting

Note:

This Exam Outline is for general use only. It does not cover all exam details.