Huawei ICT Competition 2021-2022 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 min	60	True/False Questions, 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 Types	Total Score
National Stage	Written	90 min	90	True/False Questions, Single-Choice Question and Multiple-Choice Question	1000

1.3. Network Track of Huawei ICT Competition Regional Stage Overview

Competition Stage	Exam type	Duration	Number of Questions	Question Types	Number of participants	Total Score
Regional Stage	Written	90 min	60	True/False Questions, Single-Choice Question and Multiple-Choice Question	1(Personal)	1000
	Lab	4 Hours	/	/	3(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 participants	Total Score
Global Stage	Lab	8 Hours	3(Team)	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 **include but are not limited** to the basic knowledge of Datacom, Security, and WLAN. Specific exam contents are as follows: routing protocols, Layer 2 switching technology, IPv6 technologies, Huawei firewall features, VPN technology, WLAN networking and configuration.

3.2. Knowledge to Be Tested

Datacom:

1. Datacom basics, TCP/IP protocol basics.
2. STP, RSTP and MSTP switching behavior, application and configuration.
3. TCP/IP protocol stack basics, principles of WAN (such as PPP) protocols, PPPoE implementation at the customer edge, and application of these protocols to Huawei routers.
4. Principles and application of Ethernet technologies, VLAN, Eth-Trunk, iStack.
5. Principles and application of IPv6 basics, stateless auto-configuration, DHCPv6 and IPv6 transition technology.

6. Principles and application of static route, route-policy, OSPF, OSPFv3, ISIS (IPv4), ISIS (IPv6), BGP, and BGP4+.
7. Principles and configuration of MPLS, MPLS VPN, GRE VPN, L2TP, ACL, VRRP, and BFD.
8. Principles and configuration of Telnet, FTP, DHCP.
9. Principles and configuration of programming automation, the implementation of network automation.
10. Principles and Networking of SDN, such as VXLAN, BGP EVPN, and iMaster NCE application.
11. Principles and configuration of Multicast.
12. Principles and configuration of QoS.
13. Segment Routing Principle, such as SR-MPLS and SRv6.

Security:

1. Security information and security overview, such as information security standards and specifications, basic network concepts and common network devices, common information security threats, and threat defense and information security development trends.
2. Security attack and defense technologies, such as host and OS security, web security, IPS, information collection and network detection, content security filtering technology and data security.
3. Network security basis, such as security zone, security policy, network address translation technology, dual-system hot standby and firewall user

management.

4. Application of encryption and decryption, such as encryption and decryption mechanism. PKI certificate system, and application of cryptographic technologies.
5. VPN technology such as L2TP VPN, GRE VPN, IPSec VPN, SSL VPN and L2TP over IPSec.
6. Security operation and analysis such as introduction to security operations, data monitoring and analysis, digital forensics, situation awareness and cybersecurity emergency response.
7. Advanced firewall features and networking, such as firewall intelligent uplink selection, server load balancing, bandwidth management, and virtual system.
8. Network-Layer security protection such as packet filtering, DDoS attack defense, single-packet attack defense, blacklist and whitelist and IP-MAC address binding.
9. Firewall IPv6 technologies.
10. Cloud security technology and network architecture design.

WLAN:

1. WLAN working principles and deployment.
2. WLAN topologies, 802.11 protocol, 802.11 physical layer technology, CAPWAP fundamentals.
3. WLAN configuration, roaming, two-node cluster hot backup, multicast and

security configuration.

4. WLAN location technology.
5. WLAN service quality and network optimization.
6. Wi-Fi 6 technologies and products.
7. WLAN networking, planning and design.
8. WLAN IPv6 network, IPv6 basics, network security.
9. WLAN troubleshooting.
10. CloudCampus solution, VXLAN, underlay, fabric, overlay.

Note:

The content mentioned in this article provides a general exam guide; the exam may contain additional related content that is not included here.