In cybersecurity, data protection involves safeguarding information from unauthorized access, use, disclosure, disruption, modification, or destruction, encompassing various technologies, policies, and procedures.

"data" refers to any information stored or transmitted electronically, encompassing everything from personal details to financial records, and it's a primary target for cyberattacks, requiring robust security measures to protect its confidentiality, integrity, and availability.

A network is an interconnected system of two or more computers or devices that allows for communication and sharing of resources. It can be a local area network (LAN) within a building or a wide area network (WAN) spanning across larger geographical areas.

Information is an abstract concept that refers to something which has the power to inform. At the most fundamental level, it pertains to the interpretation (perhaps formally) of that which may be sensed, or their abstractions.

Network security protects a network from unauthorized access, misuse, or attacks. It uses tools, policies, and technologies to keep data safe.

while

Cyber security is how individuals and organisations reduce the risk of cyber attack. Cyber security's core function is to protect the devices we all use (smartphones, laptops, tablets and computers), and the services we access - both online and at work - from theft or damage.

Why do you need security

New job

**Overview**

We’re looking for a Network Engineer with the proven ability to analyze and resolve hardware and software problems and troubleshoot network performance issues. The role will operate within the IT unit under the Global IT Operations Manager.

**Accelerating Progress. Securing Futures.**  
  
At TeKnowledge we help governments, businesses, and technology providers not only navigate but thrive in today’s complex technology landscape. Our services provide unparalleled value and impact to our clients across cybersecurity, advanced technical skilling, and enterprise technical support. We are committed to enabling technology, AI, CX, and security, uniquely positioning us in the market, and ensuring our customers are equipped to achieve their strategic goals.

**Responsibilities**

* Monitor, maintain, and manage all network devices globally to keep them running properly
* Establish a networking environment by designing and implementing routing devices (routers/switches) system configuration
* Secure network system by establishing and enforcing access control policies, and utilizing internet links
* Follow change control management while implementing system changes, upgrades, and updates
* Provide technical support to other teams
* Conduct Daily/ Weekly and Monthly System Health checklist, ensuring all IT Global policies/standards and procedures are in place
* Maintain safety standards in the working environment that comply with YNV Group and partner’s HSSE standard
* Make sure all Security ERs/patches/hotfixes to all network equipment
* Capacity planning for system upgrade
* Fully understand Disaster Recovery Plan (DRP) for business continuity, ensuring compliance with YNV Group’s global DRP and joining the project team for DR Exercise
* Technical Representative at his/ her site for solving Crisis problems

**Qualifications**

* Master’s Degree in Computer science, Information technology, or any related field, along with 4+ years of experience working as Network and Systems Engineer, and ITIL v3/v4 or ISO2001 (ITIL certification will be an added advantage)
* Professional fluency in English is essential, both written and spoken
* Proven experience in provisioning/administration with any vendor hypervisor (VMware ESX, Microsoft Hyper-V, Citrix Xen, others)
* Networking: general knowledge of devices, LAN/WAN concepts, data transmission, routing, protocol stack, DNS, DHCP, load balancing, firewalls
* Excellent understanding of computer systems, security, network and systems administration, databases and data storage systems, and telecommunications
* Knowledge of cloud technologies and backup software
* Strong technical skills with IPBX (VoIP), Server technology, and Virtualization
* Solid experience in IT Service Management for Incident, Change, and Configuration Management
* Excellent leadership, decision-making, project management, communication, crisis management, technical (especially in Microsoft technologies), and influencing skills
* Should be a creative and analytical team player capable of working well under pressure

Key Differences

**A bug** is an issue or flaw in software.

**A patch** is a fix for a specific issue, usually security-related.

**An update** is a broader improvement that may include patches, new features, and optimizations.

### **Difference Between Patch, Update, and Bug**

| **Term** | **Definition** | **Purpose** | **Example** |
| --- | --- | --- | --- |
| **Patch** | A small fix for security vulnerabilities, bugs, or performance issues. | Fixes specific problems, mainly security flaws. | A patch is released to fix a newly discovered vulnerability in Windows. |
| **Update** | A broader improvement that may include patches, new features, and performance enhancements. | Enhances security, adds features, and improves performance. | A software update that improves app functionality and security. |
| **Bug** | A flaw or error in the software code that causes unintended behavior. | Can cause crashes, security vulnerabilities, or performance issues. | A bug in an application causes it to crash when clicking a certain button. |

er(config)#aaa new-model

Router(config)#radius server ?

WORD Name for the radius server configuration

Router(config)#radius server cybersecurity

Router(config-radius-server)#address ipv4 10.0.0.2

Router(config-radius-server)#key 12

Router(config-radius-server)#

aaa new-model

radius server (radius name)

address ipv4 (server ip address)

key (password)

exit

aaa authentication login default group radius local

line vty 0 15

login authentication default

exit

