|  |  |  |
| --- | --- | --- |
|  |  | Adrian Simmons  **Consultant /Architect / Engineer**  **(End-to-End solutions Provider)** |
| PROFILE Over 30 years of experience in IT and Telecom Infrastructure Engineer Proving with a robust background in Infrastructure management, Network Security, and infrastructure support. Proficient in managing complex projects, including cloud migrations and network security. Demonstrated expertise in Azure, M365, and a range of networking technologies. Adept at leading teams, mentoring peers, and delivering high impact solutions in fast-paced environments.    Based in Cheltenham  **CONTACT DETAILS:**  **PHONE NUMBER:**  07756088757    **WEBSITE:**  [www.adsinet](http://www.adsinet)[-it.com](http://www.adsinet-it.com/)    **EMAIL ADDRESS:**  adrian.simmons@adsinet-it.co.uk    LinkedIn:  [linkedin.com/in/adrian-simmons-a34b8a42](https://www.linkedin.com/in/adrian-simmons-a34b8a42) HOBBIES Technology  Reading  Football  F1    **SKILLS**  **Microsoft Server Infrastructure**  **(Windows Server)**   * **Windows Server Installation and Configuration:** * **Active Directory Domain Services (AD DS):** * **Identity and Access Management:** * **Network Services Configuration:** * **Storage Management:** * **High Availability and Clustering:** * **Hyper-V Virtualization** * **Security and Compliance** * **Other Servers: DHCP, DNS, Exchange, SQL, CA, MDM, AV**   **Linux Server Infrastructure**  **(Ubuntu, CentOS, Red Hat)**   * **Linux Server Installation and Configuration:** * **Network Services Configuration:** * **Linux Security and User Management:** * **Storage and File System Management** * **Automation and Scripting:** * **Virtualization with KVM and VMware:** * **High Availability and Load Balancing:** * **Monitoring and Management:**   **VMware Virtualization**   * **vSphere and ESXi Administration:** * **VMware Security and Compliance:** * **Backup and Disaster Recovery:**   **SKILLS**  **M365 and Azure**   * **Azure Administration** * **Security** * **Azure DevOps** * **Monitoring and Management** * **Azure Cloud Solutions** * **Data and AI:** * **Azure Governance** * **Migrations** * **MDM Solutions: ABM and Intune** * **Microsoft Full Stack** * **Power BI Apps** * **Exchange Online – Powershell** * **Landing Zone** * **Kubernetes** * **AI bots** * **Hybrid Exchange** * **SharePoint** * **Dynamics356** * **SaaS, PaaS, IasS, CaaS and BaaS**   **Networking**   * **Routing and Switching** * **Network Security** * **Cisco Wireless Networking (Wi-Fi)** * **Data** * **WAN and VPN Technologies** * **Network Automation and Programmability** * **Monitoring and Troubleshooting** * **VoIP and Collaboration:**   Bottom of Form  **Telephony and VoIP**  **VoIP Architecture and Fundamentals**   * **VoIP Network Design** * **SIP Trunking** * **SIP (Session Initiation Protocol) Trunking**   **VoIP Systems Implementation**   * **PBX (Private Branch Exchange) Systems** * **Hosted VoIP/Cloud PBX**   **Unified Communications (UC)**   * **Unified Communications Integration**   **Microsoft Teams VoIP (Telephony)**   * Microsoft Teams Calling * Microsoft Teams Integration with SIP Trunks   **VoIP Security and Compliance**   * VoIP Security Best Practices * Spam Over Internet Telephony (SPIT) Protection   **Quality of Service (QoS)**   * VoIP Quality of Service * VoIP Call Monitoring and Troubleshooting   **VoIP Hardware and Endpoints**   * VoIP Phones and Devices * Analog to VoIP Conversion   **Network Management and Troubleshooting**   * VoIP Network Monitoring * VoIP Troubleshooting Tools   **VoIP Deployment in Virtualized and Cloud Environments**   * Virtual PBX Implementation * Disaster Recovery and Redundancy   **VoIP Deployment Tools and Platforms**   * Cisco Unified Communications Manager (CUCM) * Siemens * Mitel * Avaya * Asterisk * 3CX * Microsoft Teams Calling * RingCentral, Zoom Phone, eight-by-eight, Vonage   **Cyber Security**   * **Risk Assessment and Management** * **Network Security** * **Identity and Access Management (IAM)** * **Data Security and Encryption:** * **Application Security** * **Cloud Security** * **Incident Response and Threat Detection** * **Governance, Risk, and Compliance (GRC)** * **Disaster Recovery and Business Continuity** * **Cyber Security Tools and Platforms**   **Tools:**   1. **Firewalls:** Cisco ASA, Palo Alto, Fortinet, Check Point 2. **IDS/IPS:** Snort, Cisco Firepower, Palo Alto Threat Prevention 3. **EDR:** CrowdStrike, Sentinel One, Microsoft Defender 4. **SIEM:** Splunk, IBM QRadar, Microsoft Sentinel, AlienVault, ArcSight, Graylog, RSA NetWitness**,** Elastic SIEM, Securonix, SolarWinds Security Event Manager (SEM) |  | Certificates and Training  * Certified Cisco Professional (CCNP) * VMWare Certified Professional (VCP) * Certified Wireless Network Professional (CWNP) * Microsoft Certified Engineer (MCSE / MCSA) * Powershell * Rukus Reseller/Engineering Training * Barracuda Reseller/Engineering Training * Sophos Reseller/Engineering Training * And many more reseller Training Programs  Work Experinece **ADSINET LTD**  **Contracts from June 2023 – to – Present**  Companies benefited from my experience:  HSL COMPLIANCE – Support Engineer (6-Month Contract 2024)  Fortem – Barracuda data centre consultant/Engineer (6-month Contract 2024)  Simplify IT – Senior Infrastructure consultant/Engineer (3- Month Contract 2023)  Planet-IT – Project Engineer (3-month Contract 2023)  **Permanent roles:**  Accenture – Presales Cyber Security consultant (From July 2022 – June 2023)  Marathon – Senior Infrastructure technical consultant (From June 2020 to June 2022  **ADSIMPLICIY LTD**  **Contracts from Jan 2019 – to – June 2020**  GE Aviation – Network Engineer  Roof Top Housing – Senior Infrastructure Engineer  Gloucestershire Royal Hospital – Senior Project Network Engineer  **PSU Technology (Jan 2018 – Jan 2019 Permanent)**  **System architect / 3rdLine Support**  Being the third line escalation for the service desk and second line support with BAU support and the handover of projects that had completed the life cycle through process of Agile. Producing handover document of the project which included knowledge bases and running workshops. Following ISO procedure 27001 and 9003 for ITIL Change Management procedures.  Planning, developing, and supporting the following:  Platforms: On-premises, Clustered VMWare Data Centre’s v5 to 6.5, Hyper-V clusters. O365 full stack and azure cloud services including AWS.  AD (2008/2012/2016), ADFS, Exchange 2010, 2013, 2016, SharePoint, DNS, DHCP, Certificate Server, Radius SQL, MySQL, SCCM, SCOM, Citrix Servers, Citrix Zendesk. End client (Window 8/10)  Networking: Routers, Firewall – Cisco, SonicWall, Dray Tek. Switches for VLAN: Cisco, Dell, and HP  Storage for VMware and Hyper-V – Dell SAN and NAS, NetApp,  Symantec Cloud Security, Barracuda (Lead Engineer Mail Archiving) and Mime Cast. Hosting of DNS records. Sophos UTM Solutions. ASA Firewalls and Fortinet  Product owner for projects through the Agile methodology using Jira for managing the projects that have been consulted, through the Account Managers and Sales team with customer visits. Where required for the project, producing full design documentation as required by the customers who do not have a full understanding of Agile mythology.  Office 365 Migration from Exchange 2010/2013 (O365, Teams, Power Bi, SharePoint) projects for:  Recruitment business in Manchester with over one thousand employees in the UK.  Financial institution in Cheltenham for over five hundred employees.  Global logistics company based in London with over four thousand employees.  Travel Organisation based in Oxfordshire with over 1500 employee in the UK.  Lead Projects Engineer:  Exchange and O365 migrations  Azure/ASR, Network security with Firewall and Cyber Essentials.  Virtualisation for Hyper-V and VMWare datacenter  Barracuda and Sophos  Cyber Essentials Accreditation  **Vaughan Data Systems (Aug 2016 to Jan 2018 Permanent)**  **Service Manager**  Projects included IaaS, PaaS, and SaaS  Princes 2 Methodology  Managing and developing a team of engineers including being the senior escalation for BAU support. Assisting and designing the development of the sale team and senior management with existing and new customers. Managing a team of 6 Engineers and 3 Admin staff.  Project planning and producing fully designed documentation for bidding on new and existing customers on IT and Telecoms.  Lead Project Engineer on O365 Migrations and Exchange - included (End to End with full documentation):  Office 365 Migration from Exchange 2010/2013 (Inc. O365, Sky for Business, Power Bi, SharePoint) projects for:  Supporting: Symantec Cloud Security, Barracuda (Lead Engineer Mail Archiving) and Mime Cast. Hosting of DNS records. Sophos UTM Solutions. ASA Firewalls and Fortinet  Planning, developing, and supporting the following:  Platforms: On-premises, Clustered VMWare Data Centre’s v5 to 6.5, Hyper-V clusters. O365 full stack and azure cloud services including AWS.  Design and built: AD (2008/2012/2016), ADFS, Exchange 2010, 2013, 2016, SharePoint, DNS, DHCP, Certificate Server, Radius SQL, MySQL, SCCM, SCOM, Citrix Servers, Citrix Zendesk. End client (Window 8/10)  Networking: Routers, Firewall – Cisco, SonicWall, DrayTek. Switches for VLAN: Cisco, Dell, and HP  Storage for VMware and Hyper-V – Dell SAN and NAS, NetApp,  Other Projects:  Lead Projects in Azure/ASR, Network security with Firewall and Cyber Essentials.  Lead Engineer on Virtualisation for Hyper-V and VMWare data centers.  Lead Engineer on Sophos Encryption.  ASPINET Limited (From 2005 To 2016)  IT and Telecom Support Consultant  Engineer – Projects included IaaS, PaaS, and SaaS  Avaya RED Engineer.  SaaS services: Gamma, Office 365 Migrations, Horizon and many more.  NNR Global Logistics (From 1995 to 2005)  IT Controller/Manager  Running ISO 27001 processes and procedures.  Hand-on engineering and dealing with external vendors.  **Skills**  **Microsoft Server Infrastructure**  **Windows Server**   * **Windows Server Installation and Configuration:**   + Installation of Windows Server (2016, 2019, 2022)   + Server roles and features management (Active Directory, DNS, DHCP, IIS)   + Windows Server Core setup and configuration   + Group Policy management (GPO creation, deployment, and troubleshooting)   + Disk management, RAID configuration, and file system management (NTFS/ReFS) * **Active Directory Domain Services (AD DS):**   + AD DS installation, configuration, and domain controller promotion   + User, group, and organizational unit (OU) management   + Group policy creation and management (GPO)   + Domain trust relationships, forests, and multi-site AD setup   + AD replication management and troubleshooting * **Identity and Access Management:**   + Integration with Azure Active Directory (Azure AD) for hybrid environments   + Certificate Services (PKI) for secure communication   + Active Directory Federation Services (AD FS) for Single Sign-On (SSO)   + Multi-factor authentication (MFA) and Conditional Access policies   + Role-based access control (RBAC) implementation * **Network Services Configuration:**   + DHCP server setup and IP addressing management   + DNS server setup, DNS zone creation, and name resolution   + Network Policy Server (NPS) for RADIUS authentication   + VPN server setup with Routing and Remote Access (RRAS)   + IP address management (IPAM) and network troubleshooting * **Storage Management:**   + Windows Server Storage Spaces and SAN/NAS configuration   + iSCSI target and initiator setup for storage networking   + Distributed File System (DFS) for file replication and namespace management   + Data deduplication and storage tiering for efficiency   + Backup and Restore with Windows Server Backup or third-party tools (Veeam) * **High Availability and Clustering:**   + Failover clustering for high availability (HA) of critical services   + Cluster shared volumes (CSV) for Hyper-V or file server clusters   + Network Load Balancing (NLB) for web and application servers   + Active Directory site and services replication setup for redundancy   + Disaster recovery planning and execution * **Hyper-V Virtualization:**   + Installing and configuring Hyper-V role on Windows Server   + Creating and managing virtual machines (VMs)   + Virtual hard disks (VHD/VHDX) creation and management   + Virtual switches, network adapters, and VLANs setup   + Configuring live migration and VM replication for high availability   + Hyper-V failover clustering for load balancing and HA * **Security and Compliance:**   + Windows Server Update Services (WSUS) for patch management   + Windows Defender Antivirus configuration and monitoring   + BitLocker Drive Encryption for data protection   + Security baselines, audits, and compliance with CIS, NIST standards   + Implementing firewalls and network security features like IPsec   **Linux Server Infrastructure**  **Ubuntu, CentOS, Red Hat**   * **Linux Server Installation and Configuration:**   + Installation of Linux distributions (Ubuntu, CentOS, Red Hat)   + Command-line interface (CLI) configuration and management   + Package management (apt, yum, dnf) for installing/updating software   + Managing system users, groups, and permissions (chown, chmod)   + Disk partitioning, LVM setup, and file system management (ext4, XFS) * **Network Services Configuration:**   1. Configuring static IP addresses, DNS, and hostname settings   2. DHCP, DNS, and NTP server configuration   3. Network troubleshooting with tools like ifconfig, netstat, ip, and traceroute   4. SSH server configuration for secure remote access   5. Firewall setup using iptables, firewalld, or UFW (Uncomplicated Firewall) * **Linux Security and User Management:**   1. User and group management (useradd, groupadd, passwd)   2. Implementing sudo and least privilege access control   3. SELinux and AppArmor for mandatory access controls   4. Linux firewall (iptables) for securing traffic   5. SSH hardening and key-based authentication * **Storage and File System Management:**   1. Configuring RAID arrays (mdadm) and Logical Volume Manager (LVM)   2. NFS and Samba for file sharing between Linux and Windows environments   3. Disk quotas for managing storage usage   4. Mounting remote filesystems with NFS, CIFS, and SSHFS   5. Backup solutions using tar, rsync, or third-party tools (Bacula, Duplicity) * **Automation and Scripting:**   1. Bash scripting for task automation (cron jobs, scheduled tasks)   2. Ansible, Puppet, or Chef for configuration management   3. System performance monitoring and tuning using top, htop, sar, and iostat   4. Automating software deployment and system updates   5. Log management and rotation with syslog, logrotate * **Virtualization with KVM and VMware:**   1. **KVM (Kernel-based Virtual Machine):**      1. Installing and configuring KVM for Linux virtualization      2. Creating, configuring, and managing virtual machines (VMs) with virsh      3. Network bridge and NAT configuration for VMs      4. VirtIO drivers for performance optimization      5. Storage configuration using raw or qcow2 images   2. **VMware vSphere/Esxi:**      1. vCenter and Esxi host setup and configuration      2. Creating and managing VMs, templates, and resource pools      3. Configuring VMware tools for performance optimization      4. vMotion for VM migration and DRS (Distributed Resource Scheduler)      5. VMware High Availability (HA) and fault tolerance configuration      6. VMware snapshots, backups, and disaster recovery planning * **High Availability and Load Balancing:**   1. Linux clustering with Corosync and Pacemaker   2. HAProxy and NGINX for load balancing web servers   3. GlusterFS or Ceph for distributed storage and redundancy   4. Configuring and managing MariaDB/MySQL replication for HA databases   5. Heartbeat and Keepalive for failover in high-availability environments * **Monitoring and Management:**   + Installing and configuring Nagios, Zabbix, or Prometheus for server monitoring   + SNMP configuration for network management and monitoring   + Analysing system logs with journalctl, syslog, and dmesg   + Performance monitoring and tuning with top, htop, and iostat   + Implementing alerts and notifications for critical system events   **VMware Virtualization Skills**   * **vSphere and ESXi Administration:**   + Installing and configuring VMware ESXi hosts   + Managing virtual machines (VMs) in VMware vCenter   + Creating VM templates, cloning VMs, and managing snapshots   + Configuring virtual switches and VLANs for networking   + Storage management with VMware vSAN and third-party storage arrays   + vMotion, Storage vMotion, and VMware DRS for load balancing and HA * **VMware Security and Compliance:**   + Role-Based Access Control (RBAC) in vCenter   + Implementing SSL/TLS for vSphere security   + VMware vShield/NSX for network security and micro-segmentation   + VMware Log Insight for centralized log management   + Security audits and compliance using VMware’s Security Configuration Guides * **Backup and Disaster Recovery:**   + Integration with backup solutions (Veeam, Zerto)   + VMware Data Recovery (VDR) for backups and restores   + Disaster Recovery with Site Recovery Manager (SRM)   + Replication and failover planning between data centers   **M365 and Azure**   * **Azure Administration:**   + Subscription and resource management   + Virtual Machine (VM) deployment and management   + Azure Storage management (Blob, File, Table, Queue)   + Azure Virtual Networks (VNet) and networking   + Azure Resource Manager (ARM) templates * **Security:**   + Azure Security Center configuration   + Azure Key Vault (secrets, certificates, keys management)   + Azure AD Identity Protection and Privileged Identity Management (PIM)   + Role-Based Access Control (RBAC)   + Secure Access (NSG, Azure Firewall, VPN, and ExpressRoute) * **Azure DevOps:**   + Pipelines (CI/CD automation)   + Repos (source code version control)   + Infrastructure as Code (IaC) with ARM or Terraform   + GitHub integration for DevOps practices * **Monitoring and Management:**   + Azure Monitor and Log Analytics   + Application Insights for performance monitoring   + Azure Automation (runbooks, scheduling tasks) * **Azure Cloud Solutions:**   + Azure Kubernetes Service (AKS) and containerization   + Azure App Services (web apps, API apps)   + Azure Functions (serverless computing)   + Azure SQL Database and Cosmos DB   + Azure Backup and Disaster Recovery (Azure Site Recovery) * **Data and AI:**   + Azure Machine Learning   + Azure Synapse Analytics (Big Data)   + Azure Data Lake and Azure Databricks   + Azure Cognitive Services (AI and NLP capabilities) * **Azure Governance:**   + Azure Policy and Blueprint for compliance   + Cost management and billing insights   + Azure Advisor recommendations * **Migrations:**   **Planning and Assessment:**   * **Environment Discovery:**   + Assess current infrastructure (Exchange, SharePoint, file servers, etc.)   + Analyze existing workloads (email, files, applications) for compatibility.   + Identify dependencies and integrations (e.g., third-party apps, on-prem servers)   + Network readiness assessment for bandwidth and latency. * **User and Data Assessment:**   + Identify and audit users, mailboxes, file shares, and data volumes.   + Categorize data based on priority and compliance requirements.   + Assess user groups, roles, and permissions for correct mapping.   + Inventory of collaboration tools (Skype for Business, Teams, SharePoint)   **Migration Strategies and Tools:**   * **Cutover, Staged, or Hybrid Migration:**   + Determine migration type (cutover, staged, hybrid) based on business needs.   + Set up hybrid configurations with existing on-prem Exchange, SharePoint, or AD   + Plan phased migration if dealing with large or complex environments.   + Plan for coexistence between on-prem and cloud environments (mail flow, identity) * **Migration Tools:**   + **Microsoft FastTrack** for planning and guidance   + **Microsoft Migration Manager** for file migration to OneDrive and SharePoint   + **Exchange Admin Center (EAC)** for Exchange Online mailbox migrations   + **SharePoint Migration Tool (SPMT)** for moving SharePoint and file share content.   + **Third-party tools** like Bit Titan, Quest, or SkyKick for larger, complex migrations   **Exchange Online Migration:**   * **Mailbox Migrations:**   + Exchange On-Prem to Exchange Online mailbox migration (cutover, staged, or hybrid)   + Migrating public folders and distribution groups   + Configuration of DNS (MX, Autodiscover) for seamless mail flow   + Mailbox size management, archiving, and retention policies   + Calendar and contacts migration, ensuring no data loss. * **Hybrid Configuration:**   + Configuring Exchange Hybrid Mode (Exchange Hybrid Configuration Wizard)   + Secure mail flow between on-prem and cloud with connectors   + Managing hybrid mailboxes and cross-premises permissions   + Implementing DirSync/AD Connect for identity and authentication synchronisation.   **OneDrive and SharePoint Online Migration:**   * **File and Document Migration:**   + Migrating home directories and file shares to OneDrive for Business   + SharePoint site and document library migration (from SharePoint on-prem or other systems)   + Mapping shared folders and team drives to SharePoint document libraries.   + Migrating user and department file shares to SharePoint Online   + Preserving metadata, versioning, and permissions during migration * **File Collaboration and Security:**   + Setting up OneDrive and SharePoint for real-time collaboration   + Configuring conditional access and DLP (Data Loss Prevention) policies for migrated data   + Implementing OneDrive Files On-Demand for bandwidth efficiency   **Teams and Skype for Business Migration:**   * **Skype for Business to Microsoft Teams Migration:**   + Migrating chat history, contacts, and meeting data from Skype for Business to Teams   + Coexistence strategy for running both platforms during transition.   + Configuring Teams Calling (Telephony) and meeting migration * **Teams Adoption and File Sharing:**   + Migrating files and collaboration data to Teams from SharePoint, OneDrive, or third-party tools (Slack, Google Workspace)   + Setting up Teams channels, tabs, and apps for migrated data   + Enabling Teams policies for user collaboration and security compliance   **Identity and Authentication:**   * **Azure AD Connect:**   + Setting up and configuring Azure AD Connect for synchronization between on-premises Active Directory and Azure AD   + Synchronising user identities, passwords, and groups for Single Sign-On (SSO)   + Managing identity federation with Active Directory Federation Services (AD FS)   + Handling directory synchronization issues and troubleshooting sync conflicts. * **Multi-factor Authentication (MFA) and Conditional Access:**   + Enforcing MFA during and after migration for enhanced security   + Configuring conditional access based on user, location, and device compliance.   + Setting up self-service password reset (SSPR) for end-users’ post-migration.   **Security and Compliance:**   * **Data Protection and Governance:**   + Implementing M365 data loss prevention (DLP) policies post-migration   + Ensuring compliance with regulatory requirements (GDPR, HIPAA, etc.)   + Configuring retention policies and eDiscovery for legal compliance   + Setting up sensitivity labels and encryption for email and document security * **Microsoft Defender for Office 365:**   + Configuring email security to prevent phishing, spam, and malware   + Protecting documents with Defender ATP (Advanced Threat Protection)   + Post-migration audit and threat detection configuration   **Post-Migration Tasks and Optimization:**   * **End-User Training and Support:**   + Training end-users on using Outlook, Teams, OneDrive, and SharePoint in the M365 environment.   + Providing documentation and knowledge transfer for administrators and helpdesk teams   + Addressing user concerns with change management strategies * **Performance Optimization:**   + Monitoring M365 service health post-migration (Exchange, SharePoint, OneDrive)   + Addressing bandwidth, sync, and user performance issues   + Reviewing mailbox and data performance, resolving throttling issues * **Decommissioning Legacy Systems:**   + Planning for safe decommissioning of on-premises servers (Exchange, SharePoint)   + Removing old directories, disabling DNS records, and ensuring smooth cutover   + Archiving or securely disposing of legacy data is no longer needed in the cloud.   **Troubleshooting and Support:**   * **Migration Troubleshooting:**   + Resolving mailbox migration issues (stuck queues, incomplete syncs)   + Addressing file migration errors (permissions, large files, corrupted data)   + Troubleshooting Active Directory sync errors (duplicate users, conflict resolution) * **Post-Migration Support:**   + Monitoring user issues with email, files, and collaboration tools   + Identifying performance bottlenecks and resolving network latency issues   + Providing ongoing support for hybrid environments and phased migrations   **Third-Party Tools for Migration:**   * **Bit Titan MigrationWiz** – A comprehensive tool for mailbox, OneDrive, and SharePoint migrations. * **Quest On Demand Migration** – For complex migrations involving hybrid environments or tenant-to-tenant migrations. * **SkyKick** – Cloud-based automation tools for migrating email and collaboration data to M365. * **AvePoint Fly** – Specialized in content migration from SharePoint on-prem, file servers, and Google Workspace to M365.Bottom of Form   **Networking Skills:**   * **Routing and Switching:**   1. **Cisco Routers and Switches Configuration:**      1. Configuration of routers (ISR, ASR series) and switches (Catalyst, Nexus series)      2. VLAN creation and management      3. STP (Spanning Tree Protocol) and RSTP configuration      4. OSPF, EIGRP, BGP routing protocols      5. Inter-VLAN routing and Trunking      6. EtherChannel and link aggregation   2. **Routing Protocols:**      1. Static and dynamic routing configuration      2. Implementing RIP, OSPF, EIGRP, BGP      3. Route redistribution and summarization      4. Policy-based routing and access control lists (ACLs) * **Network Security:**   1. **Cisco ASA and Firepower:**      1. Configuring Cisco Adaptive Security Appliance (ASA)      2. Firepower Threat Defense (FTD) for intrusion prevention      3. Site-to-site VPN and Remote Access VPN      4. Cisco AnyConnect for secure remote access      5. Firewall policies and NAT (Network Address Translation)   2. **Cisco Identity Services Engine (ISE):**      1. Network access control (NAC) with 802.1x      2. Device profiling and posturing      3. Role-based access control (RBAC)   3. **Network Segmentation:**      1. Access control lists (ACLs)      2. Network segmentation with VLANs and VRF (Virtual Routing and Forwarding)      3. Cisco TrustSec implementation * **Cisco Wireless Networking (Wi-Fi):**   1. **Cisco Wireless LAN Controllers (WLC):**      1. Setup and configuration of WLC (AireOS and IOS-XE)      2. WLAN SSID creation and configuration      3. AP registration and configuration (Cisco Aironet, Meraki APs)      4. Configuring Layer 2/Layer 3 roaming      5. Integration of WLC with ISE for secure Wi-Fi authentication   2. **Wi-Fi Optimization and Troubleshooting:**      1. Channel and power planning for RF optimisation.      2. Wireless heatmap creation and site surveys      3. Spectrum analysis and interference management      4. Wi-Fi performance monitoring (AP performance, client metrics)   3. **Wi-Fi Security:**      1. WPA3/WPA2 Enterprise configuration with RADIUS      2. 802.1x and certificate-based authentication      3. Guest Wi-Fi configuration with captive portal      4. BYOD (Bring Your Own Device) network design.   4. **Wi-Fi Mesh Networking:**      1. Configuring Cisco FlexConnect for branch deployments      2. Configuring mesh access points for wireless backhaul * **Data Center Networking:**   1. **Cisco Nexus Switches:**      1. Configuration of Nexus 5000/7000/9000 series      2. VXLAN and VPC (Virtual Port Channel) setup      3. Fabric Path and EVPN configuration      4. FCoE (Fiber Channel over Ethernet) and SAN connectivity   2. **Software-Defined Networking (SDN):**      1. Cisco ACI (Application Centric Infrastructure)      2. APIC controller configuration and policies      3. Network automation with Python, NETCONF/RESTCONF, and Ansible      4. VXLAN overlays and multi-site ACI * **WAN and VPN Technologies:**   1. **Cisco SD-WAN (Viptela, Meraki):**      1. WAN edge device configuration (vEdge, Meraki MX)      2. Zero-touch provisioning and SD-WAN fabric setup      3. Application-aware routing and SLA-based traffic policies      4. Centralized management with vManage and Meraki dashboard   2. **VPN Configuration:**      1. IPSec VPN configuration (site-to-site and remote access)      2. MPLS VPN and VRF-lite configuration      3. DMVPN (Dynamic Multipoint VPN)      4. GRE tunnels and IPsec over GRE * **Network Automation and Programmability:**   1. **Cisco DNA Center:**      1. Intent-based networking for automation      2. Network provisioning, configuration, and monitoring.      3. Software-Defined Access (SDA) implementation   2. **Cisco APIs and Automation Tools:**      1. Using REST APIs for network automation      2. Python scripting for device configurations      3. Cisco DevNet platform for automation and programmability      4. NETCONF/RESTCONF protocols for automated device management      5. YANG data modeling * **Monitoring and Troubleshooting:**   1. **Cisco Prime Infrastructure:**      1. Network monitoring and performance analysis.      2. Device inventory and lifecycle management      3. Wireless and wired network performance metrics.   2. **Cisco Stealthwatch:**      1. Network visibility and threat detection.      2. Monitoring traffic flows for anomaly detection   3. **Cisco NetFlow and SNMP:**      1. Configuring NetFlow for traffic analysis      2. SNMP for device monitoring and alerts      3. Syslog configuration and analysis * **VoIP and Collaboration:**   1. **Cisco Unified Communications:**      1. Cisco Unified Communication Manager (CUCM) configuration      2. SIP Trunking and PSTN gateway setup.      3. Cisco IP Phones and Jabber configuration      4. QoS (Quality of Service) for voice and video traffic   2. **Cisco Webex and Collaboration Tools:**      1. Configuring Webex Meetings and Teams      2. Integration with M365 and Exchange Online      3. Video conferencing setup and monitoring |

**Telephony and VoIP Skills**

**VoIP Architecture and Fundamentals**

* **Understanding VoIP Technology:**
  + Knowledge of how VoIP works, packet-switched networks, and the principles of digitizing and transmitting voice data over IP networks.
  + Understanding of codecs like G.711, G.729, and Opus for voice compression and quality.
  + Familiarity with protocols such as SIP (Session Initiation Protocol), RTP (Real-Time Transport Protocol), and SDP (Session Description Protocol).
  + Difference between VoIP and traditional PSTN (Public Switched Telephone Network).
* **VoIP Network Design:**
  + Designing VoIP networks for optimal voice quality (QoS, latency, jitter, and packet loss considerations).
  + Implementing VLANs for voice traffic segregation from data traffic to improve performance and security.
  + VoIP bandwidth planning and optimization for different call volumes and codecs.
  + Designing and implementing failover and redundancy strategies for VoIP systems to ensure high availability.
* **2. SIP Trunking:**
* **SIP (Session Initiation Protocol) Trunking:**
  + Configuring SIP trunks to replace traditional PSTN lines for connecting to VoIP service providers.
  + Understanding SIP trunk configuration, session border controllers (SBC), and media gateways for connecting legacy systems to IP networks.
  + Monitoring and troubleshooting SIP trunk issues like registration failures, one-way audio, and dropped calls.
  + Managing SIP trunk capacity, scaling to accommodate business growth, and negotiating with providers for call handling capabilities.

**VoIP Systems Implementation**

* **PBX (Private Branch Exchange) Systems:**
  + Implementing, configuring, and managing on-premises or hosted IP PBX systems such as Cisco Unified Communications Manager (CUCM), 3CX, Asterisk, and Avaya IP Office.
  + Migrating from traditional PBX systems to VoIP-based systems, ensuring seamless call routing and feature parity.
  + Configuring advanced features like call forwarding, call parking, hunt groups, auto attendants, and interactive voice response (IVR).
* **Hosted VoIP/Cloud PBX:**
  + Configuring cloud-based VoIP solutions like RingCentral, Microsoft Teams Calling, Zoom Phone, and eight-by-eight.
  + Managing cloud telephony platforms, provisioning users, and configuring features such as voicemail, call queues, and call routing.
  + Ensuring security in cloud VoIP solutions (encryption of voice traffic, multi-factor authentication, and compliance).

**Unified Communications (UC)**

* **Unified Communications Integration:**
  + Integrating VoIP systems with unified communication platforms like Microsoft Teams, Skype for Business, Cisco WebEx, and Zoom for voice, video, and messaging.
  + Configuring presence features, voicemail to email integration, call forwarding between devices (desk phones, mobile, softphones).
  + Integration with CRM systems for call logging, analytics, and customer support.
  + Enabling collaboration tools like video conferencing, screen sharing, and chat within VoIP platforms.

**Microsoft Teams VoIP (Telephony)**

* **Microsoft Teams Calling:**
  + Configuring Microsoft Teams Calling (Phone System) for cloud-based telephony.
  + Direct routing configuration for integrating existing telephony infrastructure with Microsoft Teams via session border controllers (SBC).
  + Managing number porting, emergency calling (E911), and dial plans for Teams users.
  + Configuring calling policies, call queues, auto attendants, and voicemail within the Teams Admin Center.
* **Microsoft Teams Integration with SIP Trunks:**
  + Implementing direct routing to enable Microsoft Teams as a softphone integrated with SIP trunks and external PSTN systems.
  + Managing Microsoft Teams-certified devices (headsets, desk phones, speakerphones) for users.

**VoIP Security and Compliance**

* **VoIP Security Best Practices:**
  + Implementing encryption (SIP-TLS, SRTP) to secure signaling and media streams.
  + Configuring firewalls, SBCs (Session Border Controllers), and intrusion detection systems to protect VoIP infrastructure.
  + Mitigating threats like eavesdropping, call hijacking, and DoS (Denial of Service) attacks on VoIP systems.
  + Applying compliance with regulations like GDPR, HIPAA, and PCI DSS for handling VoIP traffic securely.
* **Spam Over Internet Telephony (SPIT) Protection:**
  + Implementing anti-SPIT measures to prevent unwanted or malicious VoIP calls.
  + Managing access control lists (ACLs) and call filtering to prevent unauthorized use of VoIP services.

**Quality of Service (QoS)**

* **VoIP Quality of Service:**
  + Configuring QoS policies to prioritize VoIP traffic over other types of network traffic (using DSCP, CoS, or IP Precedence).
  + Managing network traffic shaping and policing to reduce latency, jitter, and packet loss for VoIP calls.
  + Using WAN optimization techniques to ensure call quality over wide area networks.
* **VoIP Call Monitoring and Troubleshooting:**
  + Monitoring VoIP quality with tools like MOS (Mean Opinion Score), packet loss statistics, and jitter buffers.
  + Using call analytics platforms for monitoring voice traffic, dropped calls, and identifying potential issues with call quality.

**VoIP Hardware and Endpoints**

* **VoIP Phones and Devices:**
  + Configuring and managing IP phones, softphones, and SIP endpoints from vendors like Cisco, Polycom, Yealink, and Grandstream.
  + Managing user device provisioning, firmware updates, and troubleshooting device-specific issues (e.g., handset echo, latency).
  + Setting up conference phones, video conferencing endpoints, and mobile VoIP apps.
* **Analog to VoIP Conversion:**
  + Implementing analog telephone adapters (ATAs) to connect legacy analog devices (fax machines, door entry systems) to IP networks.
  + Configuring media gateways to allow seamless communication between analog PSTN and VoIP networks.

**Network Management and Troubleshooting**

* **VoIP Network Monitoring:**
  + Monitoring VoIP infrastructure using tools like SolarWinds VoIP & Network Quality Manager, PRTG, and Wireshark.
  + Configuring SNMP monitoring for VoIP system health, call quality, and bandwidth usage.
  + Troubleshooting common VoIP issues such as one-way audio, echo, dropped calls, jitter, and latency using packet captures and call logs.
* **VoIP Troubleshooting Tools:**
  + Using Wireshark for packet capture and deep-dive analysis of SIP signaling and RTP media streams.
  + Configuring and using RTCP and SIP response codes for diagnosing and fixing call quality issues.
  + Network analysis with tools like ping, traceroute, and iperf to identify network issues affecting VoIP performance.

**VoIP Deployment in Virtualized and Cloud Environments**

* **Virtual PBX Implementation:**
  + Deploying PBX systems like Asterisk, FreePBX, or 3CX in virtualized environments (Hyper-V, VMware).
  + Configuring and managing cloud-based VoIP PBX systems (e.g., AWS-hosted 3CX, Asterisk on Azure).
  + Scalability planning and resource allocation for VoIP in cloud/virtual environments.
* **Disaster Recovery and Redundancy:**
  + Implementing disaster recovery plans for VoIP systems, including backup SIP trunks and failover PBX instances.
  + Configuring high availability (HA) for VoIP servers and maintaining uptime during network or system failures.

**VoIP Deployment Tools and Platforms**

* **Cisco Unified Communications Manager (CUCM)** – Cisco’s VoIP and unified communications platform for enterprises.
* **Asterisk** – An open-source VoIP PBX platform for highly customizable telephony systems.
* **3CX** – A popular IP PBX that offers a range of VoIP telephony features with an easy-to-use interface.
* **Microsoft Teams Calling** – A cloud-based telephony system integrated with the Microsoft 365 ecosystem.
* **RingCentral, Zoom Phone, 8x8, Vonage** – Leading hosted/cloud-based VoIP platform.

**Cyber Security Skills:**

**Risk Assessment and Management:**

* **Risk Identification and Analysis:**
  + Identifying vulnerabilities, threats, and risks to IT infrastructure, applications, and data.
  + Performing regular security assessments, audits, and penetration tests.
  + Conducting business impact analysis (BIA) and risk assessments for potential security threats.
* **Risk Mitigation Strategies:**
  + Implementing risk mitigation strategies and controls (technical, administrative, and physical).
  + Using frameworks like NIST Cybersecurity Framework, ISO/IEC 27001, and CIS Controls to manage risks.
  + Establishing policies for risk acceptance, avoidance, transference, or mitigation.

**Network Security:**

* **Firewall Management:**
  + Configuring and managing firewalls (Cisco ASA, Palo Alto, Fortinet, Check Point) to protect network perimeters.
  + Implementing stateful packet inspection, next-generation firewall features, and firewall rules.
  + Enabling virtual private networks (VPNs) for secure remote access (IPsec, SSL VPNs).
* **Intrusion Detection and Prevention Systems (IDS/IPS):**
  + Configuring and maintaining IDS/IPS systems like Snort, Cisco Firepower, and Palo Alto Threat Prevention.
  + Analyzing network traffic and detecting suspicious activities or anomalies.
  + Responding to alerts and preventing or mitigating identified intrusions.
* **Segmentation and VLANs:**
  + Designing and configuring network segmentation to isolate sensitive assets from the general network.
  + Using VLANs to control and manage traffic flow, improving security and reducing attack surfaces.
  + Implementing software-defined networking (SDN) and micro segmentation for dynamic network isolation.

**Endpoint Security:**

* **Antivirus and Endpoint Detection and Response (EDR):**
  + Deploying and managing antivirus and anti-malware solutions across devices (Trend Micro, Symantec, McAfee).
  + Implementing EDR solutions like CrowdStrike, Sentinel One, or Microsoft Defender for advanced threat detection and response.
  + Conducting real-time monitoring and analysis of endpoint behavior to detect malicious activity.
* **Patch Management:**
  + Implementing automated patch management systems to ensure that software and hardware are up to date.
  + Identifying and addressing vulnerabilities through timely updates (Windows, Linux, third-party applications).
* **Device Hardening:**
  + Configuring and enforcing security policies for endpoint devices (desktops, laptops, mobile devices).
  + Disabling unused ports, applying least-privilege principles, and securing boot processes.
  + Ensuring encryption of devices and storage (BitLocker, FileVault, VeraCrypt).

**Identity and Access Management (IAM):**

* **Access Control Policies:**
  + Implementing role-based access control (RBAC) and attribute-based access control (ABAC).
  + Configuring access policies using directory services like Active Directory (AD), Azure AD, or LDAP.
  + Applying the principle of least privilege (PoLP) and enforcing privileged access management (PAM).
* **Multi-Factor Authentication (MFA):**
  + Enabling and managing MFA for user authentication across critical systems and applications.
  + Configuring MFA platforms like Duo, Okta, Microsoft Authenticator, or Google Authenticator.
  + Protecting credentials and reducing the risk of unauthorized access with MFA tokens, biometric, and device-based authentication.
* **Single Sign-On (SSO):**
  + Implementing SSO for simplified and secure access to multiple applications.
  + Configuring identity federation with SAML, OAuth 2.0, OpenID Connect, and Azure AD.

**Data Security and Encryption:**

* **Encryption and Key Management:**
  + Configuring and managing encryption for data at rest, in transit, and in use.
  + Using encryption protocols such as SSL/TLS, IPsec, and AES for secure communication and data protection.
  + Implementing key management systems (KMS) for secure handling of cryptographic keys and certificates (PKI, HSMs).
* **Data Loss Prevention (DLP):**
  + Configuring DLP solutions (Symantec, McAfee, Microsoft Defender) to prevent sensitive data leakage.
  + Monitoring data flows and enforcing policies to detect and block unauthorized data transfer.
  + Applying DLP policies for email, file shares, cloud storage (OneDrive, SharePoint), and endpoint devices.
* **Database Security:**
  + Securing databases through encryption, access control, and auditing (SQL, Oracle, MySQL).
  + Applying security patches and managing vulnerabilities in database management systems (DBMS).
  + Using database activity monitoring (DAM) to identify and prevent malicious database activity.

**Application Security:**

* **Secure Software Development Life Cycle (SDLC):**
  + Integrating security into the SDLC through practices like threat modeling, secure coding, and vulnerability scanning.
  + Implementing secure development standards (OWASP Top 10) and using tools like SAST (Static Application Security Testing) and DAST (Dynamic Application Security Testing).
  + Performing code reviews and addressing vulnerabilities such as SQL injection, XSS, and buffer overflows.
* **Web Application Firewalls (WAF):**
  + Deploying WAF solutions (e.g., AWS WAF, Cloudflare, Imperva) to protect web applications from threats like injection attacks and DDoS.
  + Configuring security rules to block malicious HTTP requests and monitor web traffic patterns.
  + Logging and analyzing WAF activity to detect and respond to attacks.

**Cloud Security:**

* **Cloud Security Best Practices:**
  + Securing cloud infrastructure on platforms like AWS, Azure, or Google Cloud by enforcing least privilege, MFA, and encryption.
  + Implementing cloud-native security controls (AWS GuardDuty, Azure Security Center, Google Cloud Security Command Center).
  + Managing secure identity and access management, ensuring proper configurations for S3 buckets, storage accounts, and virtual machines.
* **Cloud Workload Protection:**
  + Deploying cloud workload protection platforms (CWPP) to secure applications and services across multiple clouds.
  + Implementing security policies for virtual machines, containers (Kubernetes), and serverless environments.
* **Cloud Compliance and Governance:**
  + Ensuring compliance with cloud security frameworks (CIS Benchmarks, NIST SP 800-53) and regulatory standards (GDPR, HIPAA).
  + Monitoring and managing cloud security posture with tools like Azure Policy, AWS Config, or Google Cloud Policy Intelligence.

**Incident Response and Threat Detection:**

* **Incident Response:**
  + Developing and executing incident response plans (IRP) to manage security breaches and minimize damage.
  + Utilizing Security Information and Event Management (SIEM) tools like Splunk, LogRhythm, or Microsoft Sentinel for real-time threat detection and response.
  + Conducting root cause analysis (RCA) and post-incident reviews to improve future security posture.
* **Forensic Investigation:**
  + Conducting digital forensics to gather evidence and analyse compromised systems.
  + Using forensic tools like EnCase, FTK, or Autopsy to investigate data breaches, malware infections, or insider threats.
  + Preserving the integrity of data and chain-of-custody for legal or regulatory reporting.
* **Threat Intelligence and Hunting:**
  + Leveraging threat intelligence platforms (TIPs) to collect, analyses, and respond to emerging cyber threats.
  + Conducting threat hunting to proactively search for adversaries and mitigate potential attacks before they occur.
  + Utilizing machine learning and behavioral analytics to detect advanced persistent threats (APTs).

**Governance, Risk, and Compliance (GRC):**

* **Policy and Compliance Management:**
  + Developing and maintaining security policies and procedures that comply with industry standards and regulations (ISO 27001, NIST, GDPR, HIPAA).
  + Performing security audits and assessments to verify adherence to compliance standards.
  + Creating governance structures for security, ensuring roles, responsibilities, and accountability are clearly defined.
* **Vulnerability Management:**
  + Performing regular vulnerability scanning with tools like Qualys, Nessus, or OpenVAS.
  + Prioritizing and remediating vulnerabilities based on risk severity and impact.
  + Managing patch cycles and ensuring timely resolution of critical vulnerabilities.
* **Security Awareness Training:**
  + Conducting regular security awareness training for employees to recognize phishing, social engineering, and other attack vectors.
  + Promoting a security-first culture within the organization to mitigate human error as a security risk.

**Disaster Recovery and Business Continuity:**

* **Disaster Recovery (DR) Planning:**
  + Developing and testing disaster recovery plans to ensure business continuity in the event of cyberattacks or system failures.
  + Implementing backup strategies, replication, and failover mechanisms to minimize downtime.
  + Testing DR plans regularly and updating them based on changes in the business or IT infrastructure.
* **Business Continuity Planning (BCP):**
  + Identifying critical business processes and systems and developing strategies to ensure their continued operation during a crisis.
  + Implementing automated failover solutions to recover from cyberattacks or hardware failures rapidly.

**Cyber Security Tools and Platforms:**

1. **Firewalls:** Cisco ASA, Palo Alto, Fortinet, Check Point
2. **IDS/IPS:** Snort, Cisco Firepower, Palo Alto Threat Prevention
3. **EDR:** CrowdStrike, Sentinel One, Microsoft Defender
4. **NESSUS:** Penetration testing
5. **Kali Linux –** NMAP, Burp suite, BASH