

IT Engineer

- [Interview Cheat Sheet](#)
- [Microsoft Entra](#)
- [Network Devices](#)
- [Scenario 1: User Cannot Log into M365](#)
- [Network Subnetting](#)

Interview Cheat Sheet

- Scope: Who is affected?
- Impact: How severe is it?
- Change: What changed recently?
- Authentication: How do they login?
- Connectivity: Can they reach the service?
- Service Health: Is the service actually running?
- Evidence: What do logs show?
- Fix: Implement one change at a time.
- Verify: Confirm restoration.
- Document: Record root cause and resolution.

Scenario 1: User unable to log into Microsoft 365

- What is the error message?
- Is anyone else impacted?
- Did you recently change your password?
- Where are you connecting from?
- Is this the first time you have seen this error? when did it start?
- When was the last time you were able to successfully log in? Have you returned from a break?

Microsoft Entra

Entra ID

- Cloud based identity and access management service that provides authentication, policy enforcement, and protection for users, devices, apps, and resources

Identity & Access Management (IAM)

- Ensures that the right people, machines and software components access the right resources at the right time

Entra Domain Services

- Two Windows Server Domain Controllers are deployed as part of a replica set
- These are fully managed by Microsoft and handles availability, backups and encryption
- A managed domain is configured to perform a one-way synchronisation from Microsoft Entra ID
- Users, groups and credentials from Entra ID are made available in the managed domain so that applications, services and VMs in Azure can use familiar AD DS capabilities such as domain join, GPO, LDAP, and Kerberos/NTLM authentication
- In hybrid environments, identity information from on-prem AD DS is synchronised to Microsoft Entra ID, and then made available to the managed domain
- Domain services works with both cloud-only Microsoft Entra tenants, and tenants synchronised with an on-prem AD DS environment

Network Devices

Cisco Devices

Modes :

- > User (basic access)
- # Privileged (run show commands)
- (config)# (config changes)

S1> enable	
S1# configure terminal	
S1(config)# vlan 10	
S1(config-vlan)# name SALES	
S1(config-vlan)# exit	
S1(config)# end	
S1#	
S1# show vlan	
R1# show run	
S1# show ip interface brief	
S1# show interfaces	

- Device configuration such as hostname is stored in running config
- To save, "copy running-config startup-config"

ICMP PDU (Ping Simulation)

PC (Office Admin) > SW (Office SW1) > Printer0

1. Last: (Blank), At: Office-Admin (ICMP)

- Outbound:
 - Layer 3:
 - ICMP echo request
 - Source IP = unspecified, device sets to port's IP
 - Destination IP in same subnet, device sets next hop to destination IP
 - Layer 2:
 - Next hop = unicast, looks it up in ARP table
 - Found in ARP, ARP process sets frame destination accordingly
 - Layer 1:
 - FastEthernet0 sends the Frame

2. Last: Office-Admin, At: Office-SW1 (ICMP)

- Inbound:
 - Layer 1:
 - Receives Frame

- Layer 2:
 - Frame source MAC address not in MAC table, adds it
 - (Unicast Frame) look up Destination MAC address in MAC table
- Outbound:
 - Layer 2:
 - Not in table, Floods frame to all ports in VLAN except inbound
 - Layer 1:
 - Ports 1, 2, 3, 4, 5, 6 send Frame

3. Last: Office-SW1, At: Office-R1 (ICMP)

- Inbound:
 - Layer 1:
 - Receives Frame on G0/0/0
 - Layer 2:
 - Subinterface G0/0/0.20 accepts from this VLAN
 - Frame destination MAC does not match receiving port's MAC
 - Drops the Frame

4. Last: Office-SW1, At: Printer0 (ICMP)

- Inbund:
 - Layer 1:
 - Receives Frame on FE0
 - Layer 2:
 - Frame Destination MAC = receiving port's MAC
 - De-capsulate PDU from the Frame
 - Layer 3:
 - Packet Destination IP = Device Destination IP
 - De-capsulate Packet, identifies ICMP, processes it
 - Identifies as Echo request message
- Outbound:
 - Layer 3:
 - ICMP process sends Echo reply
 - Destination IP = same subnet, sets next hop to Destination IP
 - Layer 2:
 - Next hop = unicast, looks it up in ARP table
 - Found in ARP, ARP sets Frame desination MAC to the same
 - Encapsulates PDU into Frame
 - Layer 1:
 - FE0 sends Frame

5. Last: Printer0, At: Office-SW1 (ICMP)

- Inbound:
 - Layer 1:
 - GE1/0/17 Receives Frame
 - Layer 2:
 - Frame source MAC is not in MAC table, adds it
 - Unicast Frame, looks up destination MAC in table
- Outbound:
 - Layer 2:
 - Outgoing port = access port
 - Switch sends the frame out of that port
 - Layer 1:
 - GE1/0/19 sends the Frame

6. Last: Office-SW1, At: Office-Admin (ICMP)

- Inbound:
 - Layer 1: FE0 Receives Frame
 - Layer 2:
 - Frame destination MAC = Receiving port MAC
 - Decapsulates Frame
 - Layer 3:

- Packet destination IP = device IP
- decapsulates Packet
- Identifies ICMP Packet
- ICMP process received Echo reply message

Scenario 1: User Cannot Log into M365

A user calls saying they cannot access outlook, teams or sharepoint. They receive a login error

- What is the error message?
- Is anyone else impacted?
- Did you recently change your password?
- Where are you connecting from?
- Is this the first time you have seen this error? when did it start?
- When was the last time you were able to successfully log in? Have you returned from a break?

Network Subnetting

Cheat Sheet

Group Size	128	64	32	16	8	4	2	1
Subnet	128	192	224	240	248	252	254	255
CIDR (4o)	/25	/26	/27	/28	/29	/30	/31	/32
3rd octet	/17	/18	/19	/20	/21	/22	/23	/24
2nd octet	/9	/10	/11	/12	/13	/14	/15	/16
1st octet	/1	/2	/3	/4	/5	/6	/7	/8

1. Use CIDR/Mask to find group size above
2. Starting from 0, or the corresponding subnet value above, or one to its left, increase or decrease by the group size, until you pass the corresponding octet value in the target IP
 1. Next Network ID cannot contain 256, instead increment the preceding octet by 1 and reset to 0
 2. If this is the 1st octet, Next Network is N/A, and Broadcast IP = 255.255.255.255
3. Number before target IP = Network ID
4. First Host = Network ID + 1
5. Number after target IP = Next Network ID
6. Broadcast = Next Network - 1
7. Last Host = Next Network - 2
8. #IP Addresses = Group size, or $2^{(32-\text{CIDR})}$ for 3rd/4th octet

Network ID	
First Host IP	
Last Host IP	
Broadcast IP	
Next Network ID	
No. IP Addresses	
CIDR/Subnet Mask	

- Each subnet bit doubles the available subnets
- Each host bit doubles the available host addresses

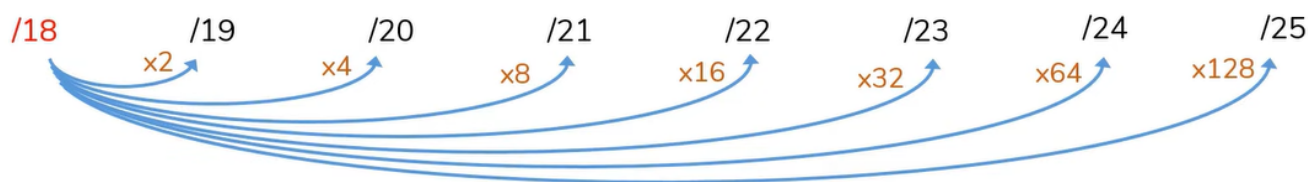
FLSM Questions

2^1	2
2^2	4
2^3	8

2^4	16
2^5	32
2^6	64
2^7	128
2^8	256
2^9	512

Starting with /18, what size sub-network would you need to create 100 sub-networks? /25

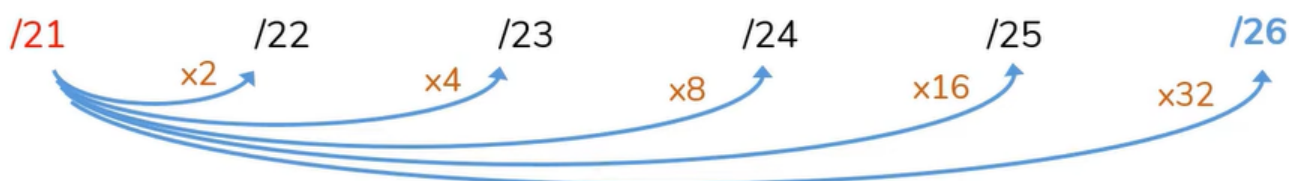
- Or, $128 = 2^7 / 18 + 7 = /25$



Starting with /21, how many sub-networks could you create that could contain 50 IP addresses? 32

- Or, $/26 - /20 = 2^5 = 32$

Group Size	128	64	32	16	8	4	2	1
Subnet	128	192	224	240	248	252	254	255
CIDR	/25	/26	/27	/28	/29	/30	/31	/32



How to Read a Subnetting Question

You will generally be given 2, and your job will be to solve the 3rd.

- A starting network size
- Number of Sub-Networks
- Size of Sub-Network

Variable Length Subnet Masks (VLSM)

<https://www.youtube.com/watch?v=amKyfbg5G2Q>