**• What is SOHO network?**

* SOHO network ka matlab he small office/home office network.

Example :-

* Chhoti company or ghar ke office ke liye network.
* Kam devices (compter,printer,mobile) connect hote he.
* Asaan or sasta setup hota he.
* Internet router se manage kiya jata he.

**• What is NAT?**

* NAT ka full form hai Network Address Translation.
* NAT ek process hai jo private IP address ko public IP address me convert karta he.
* Jab internet use karte hain to NAT ke through data safely transfer hota hai.
* Router ya firewall NAT ka use karta hai.
* Isse network secure aur IP address bachane me madad milti hai.

**• What is PAT?**

* PAT ka full form hai Port Address Translation.
* PAT ek type ka NAT hai.
* Ek hi public IP address ke saath multiple private IP devices internet use kar sakte hain.
* Har device ko alag-alag port number assign hota hai.
* Isse IP addresses bachte hain aur secure connection banta hai.

**• Different between NAT & PAT?**

* NAT
* NAT ka full form hai Network Address Translation.
* Sirf IP address ko translate karta hai.
* Har private IP ke liye alag public IP assign kar sakta hai.
* Mostly small network me use hota hai.

Example: 192.168.1.10 ko 203.0.113.5 public IP me badla.

* PAT
* PAT ka full form hai Port Address Translation.
* IP address ke saath-saath port number bhi translate karta hai.
* Sab devices ke liye ek hi public IP use hoti hai, bas port number alag hota hai.
* Jab ek public IP se kai devices internet use karte hain, tab PAT use hota hai.

Example: 192.168.1.10:1025 aur 192.168.1.11:1026 dono 203.0.113.5 IP se connect hote hain, lekin port alag he.

**• What Is Acl?**

* ACL ka full form hai Access Control List.
* ACL ek rule ka set hota hai jo network traffic ko allow ya deny karta hai.
* Router ya firewall par ACL lagaya jata hai.
* Isse decide hota hai kaun sa traffic andar aayega ya bahar jaayega.
* Security badhane ke liye ACL use hota hai.

Example:

* "192.168.1.5 IP wale computer ko internet access allowed hai, baki sabko denied."

**• What Are Different Types of Acl? What Is Wildcard Mask?**

* Types of ACL

1. Standard ACL

* Source IP address check karta he.
* Simple or basic hota he.
* Example:- 192.168.1.5 wale device ko allow karo baki sabko deny karo.

1. Extended ACL

* Source IP, destination IP, protocol (TCP/UDP) port number sab check karta he.
* Jyada control deta he.
* Example:- 192.168.1.5 se 10.0.0.5 IP par sirf HTTP (port 80) traffic allow kare.
* Wildcard mask kya hota he?
* Wildcard mask ek special number hota he jo batata he ki ACL me kaunsi IP address ko match karna he or kaunsi ignore karni he.
* Wildcard mask IP address ka opposite hota he (subnet mask ka ulta logic).
* Wildcard me 0 ka matlab exact match aur 1 ka matlab ignore.
* Example:-
* IP: 192.168.1.0
* Subnet mask : 255.255.255.0
* Wildcard mask : 0.0.0.255

**• Explain Circuit switching**

* Jab do devices (jaise phone ya computer) communicate karte hain, to Circuit Switching me ek pura dedicated path banaya jata hai un dono ke beech.
* Jab tak communication chalu hai, wo path kisi aur ke liye use nahi hota.
* Jaise purane landline telephone calls me hota tha.
* Important Points:
* Ek baar connection establish hone ke baad pura data same path se jata hai.
* Connection end hone ke baad hi wo path free hota hai.
* Delay kam hota hai, lekin network resources waste hote hain agar data continuously nahi bheja jaye to.
* Example:

Jab aap purane zamane me landline se call karte the, to aapka aur saamne wale ka ek dedicated line banta tha.

**• What is difference between leased line and broadband?**

* Leased Line
* Yeh ek dedicated private connection hota hai.
* Speed fix aur constant rehti hai.
* Mehenga hota hai.
* Mostly businesses use karte hain.
* 24x7 same performance deta hai.
* Direct connection ISP se hota hai.
* Broadband
* Yeh ek shared public connection hota hai.
* Speed kabhi tez kabhi slow hoti hai (depending on users).
* Sasta hota hai.
* Ghar ke users (home users) use karte hain.
* Peak time (evening) par speed slow ho sakti hai.
* Shared connection hota hai ISP ke network ke saath.

Simple Example:

Leased Line jaise aapka personal road - sirf aap hi use kar sakte ho.

Broadband jaise ek public road - sab log ek sath use karte hain.

**• Difference between a POTS line and a leased line?**

* Difference between POTS line and Leased line (simple words ma):

POTS Line:

* Full form: Plain Old Telephone Service.
* Sirf voice call mate hoy che (normal telephone line).
* Copper wire thi kaam kare che.
* Connection call karta hoy tyare active thay che.
* Mostly ghar na landline phone mate vapray che.
* Slow ane basic service che.
* Leased Line:
* Full form: Leased Line (special private line).
* Data, voice, ane video badhu transfer kare che.
* Fiber optic ya dedicated cable vapray che.
* Connection 24x7 active hoy che.
* Mainly companies use kare che internet ane private communication mate.
* Fast, reliable ane dedicated service hoy che.

Simple Example:

* POTS Line: Jaise aapka normal ghar ka landline phone.
* Leased Line: Jaise company ka high-speed internet connection jo sirf unka apna hota hai.

**• Practice on printer sharing**

* Computer ne Printer Connect karo
* Pela tame printer ne ek computer ke laptop sathe USB ya network thi connect karo.

2. Printer Install karo

* Driver install karo, ane check karo ke printer properly print kare chhe ke nai.

3. Printer Share Setting ON karo

* Computer par "Control Panel" kholo.
* "Devices and Printers" ma jao.
* Tame je printer connect karelo hoy te par right-click karo ane "Printer Properties" kholo.
* "Sharing" tab par jao.
* "Share this printer" par tick mark karo.
* Printer name aapi share karo.

4. Network par Sharing Enable karo

* "Control Panel" → "Network and Sharing Center" kholo.
* "Change advanced sharing settings" jao.
* "Turn on file and printer sharing" option ON karo.

5. Bija Computer par Printer Add karo

* Jene printer share karvanu hoy te computer par "Control Panel" → "Devices and Printers" kholo.
* "Add a printer" par click karo.
* "Network Printer" search karo.
* Shared printer dekhay to select karo ane install karo.

6. Print Test Page karo

* Check karo ke biju computer printer thi properly print kare chhe ke nai.

Important Points:

* Dono computers same network (Wi-Fi ya LAN) par hova joie.
* Sharing karva mate firewalls ma printer sharing allowed hovu joie.

**• Use of IIS**

* IIS ka full form hai Internet Information Services.

1. Website host karne ke liye – IIS ki madad se hum apni website ko internet ya local network par host kar sakte hain.
2. Web application chalane ke liye – ASP.NET, PHP jaise technologies se bani web applications ko IIS par run kar sakte hain.
3. FTP server ke roop mein – IIS mein FTP service bhi hoti hai, jisse files ko upload ya download kiya ja sakta hai.
4. Security ke liye – IIS SSL certificates ka support deta hai, jisse website HTTPS ke through secure hoti hai.
5. Load balancing ke liye – Jab traffic jyada hota hai to IIS load balancing ke zariye website ko smoothly chalata hai.
6. Logging aur monitoring ke liye – IIS visitors ka data, traffic analysis aur error tracking ke liye log files banata hai.
7. Authentication aur Authorization ke liye – IIS user access control karne ke liye authentication methods provide karta hai.

**• Create FTP server ,**

1. FTP Software Install karo (agar IIS nahi use karna)

* Light FTP servers jaise
* FileZilla Server (Free aur easy)
* Core FTP Server
* Download karo aur install karo.

2. Setup FTP Server

* Install karne ke baad FTP Server open karo.
* Ek New User Account banao
* Username aur Password set karo.
* Ek Shared Folder define karo
* Jise users access kar sakenge.

3. Firewall Settings

* Windows Firewall mein Port 21 ko allow karo.
* Agar Passive Mode use karte ho to extra ports open karne padenge (example: 5000-5100).

4. Test FTP Server

* Dusre computer par jaake FTP client (jaise FileZilla Client) se connect karo:
* ftp://server-ip-address
* Username/password daalke connect karo.

Note:

* FTP Port: 21
* FTP local network mein ya internet par kaam kar sakta hai.
* Secure FTP ke liye "FTPS" ya "SFTP" ka use karna better hai.

**• What is the difference between cloud and virtualization?**

* Difference between Cloud and Virtualization:
* Cloud
* Cloud ek service hai jo internet ke through computing resources (jaise servers, storage, databases) provide karti hai.
* Example: Google Cloud, AWS, Microsoft Azure
* Cloud mein aapko resources on-demand milte hain aur remote access hota hai.
* Cloud provider hardware, software aur maintenance sab handle karta hai.
* Pay-as-you-go model (jitna use utna paisa).
* Zyada scalable aur flexible hai.
* Internet hona zaruri hai.
* Virtualization
* Virtualization ek technology hai jo ek physical hardware ko divide karke multiple virtual machines banati hai.
* Example: VMware, Hyper-V, VirtualBox
* Virtualization mein ek machine par hi alag-alag virtual machines create hoti hain.
* Virtualization mein aapko khud apne physical server aur VMs manage karni padti hai.
* Mostly aap khud setup karte ho, cost fixed ya one-time hoti hai.
* Limited scalability hoti hai (jitna hardware strong utni VM banegi).
* Local system par bhi virtualization kar sakte ho.

**Virtualization** matlab ek computer ke andar chhoti-chhoti alag computers (VMs) banana.

**Cloud** matlab kisi aur ke computer (server) ko internet ke through use karna, bina apna system manage kiye.

**• Why are network monitoring tools used?**

* Network Monitoring Tools ka use hota hai

1. Network ki health check karne ke liye

Tools dekhte hain ki network devices (router, switch, server, etc.) sahi se kaam kar rahe hain ya nahi.

1. Problems jaldi pakadne ke liye

Jab network slow ho ya koi device down ho jaaye to tools turant alert bhejte hain.

1. Performance monitor karne ke liye

Network ka speed, bandwidth usage, latency (delay) wagaira continuously monitor hota hai.

1. Security issues detect karne ke liye

Agar koi unknown device connect ho ya koi unusual activity ho to tools alert dete hain.

1. Downtime kam karne ke liye

Problem aane se pehle ya turant baad pata chal jaata hai, isliye jaldi solution milta hai.

1. Network traffic analyze karne ke liye

Kaunsa device kitna data use kar raha hai, kahan bottleneck aa raha hai, yeh sab pata chalta hai.

1. Reports aur auditing ke liye

Tools detailed reports banate hain jo management ko dikhane ke liye useful hote hain.

**• What is ping ?**

* Ping ek network command hai jo check karta hai ki ek device (computer, server, website) network par reachable hai ya nahi.
* Jab hum ping command chalate hain, to humara system ek small packet send karta hai aur wait karta hai reply ka.
* Agar reply aata hai, to connection sahi hai.
* Agar reply nahi aata, to ya to device down hai ya network problem hai.
* Ping ka use:
* Network connection test karne ke liye
* Device online hai ya nahi dekhne ke liye
* Response time (delay) check karne ke liye
* Example:
* Command Prompt (CMD) mein likho:
* ping google.com
* Output mein reply time (in milliseconds) dikhega.

**• What is traceroute ?**

* Traceroute ek network command hai jo batata hai ki data (packet) aapke computer se destination (jaise website server) tak kaise travel karta hai, aur beech mein kaun-kaun se devices (routers) se pass hota hai.
* Ye har ek step (hop) ka record karta hai aur dikhaata hai ki har router tak pahuchne mein kitna time lag raha hai.
* Traceroute ka use:
* Network problem kahan ho rahi hai woh find karne ke liye.
* Kis-kis path se data jaa raha hai woh dekhne ke liye.
* Slow connection ya timeout ka reason find karne ke liye.
* Example:
* Command Prompt (CMD) mein type karo:
* tracert google.com

Important:

Windows mein command hai tracert

Linux/Mac mein command hai traceroute

**• What is nslookup?**

* nslookup ek network command hai jo kisi domain name ka IP address find karta hai, ya kisi IP address ka domain name find karta hai.

(NS ka matlab hota hai: Name Server)

nslookup ka use:

* Website ka actual IP address check karne ke liye.
* DNS (Domain Name System) problems diagnose karne ke liye.
* Kisi domain ka DNS record dekhne ke liye (jaise A record, MX record, etc.).

Example:

* Command Prompt (CMD) mein type karo:
* nslookup google.com
* Output mein google.com ka IP address aayega.

**• Explain core switches**

* Core Switches network ka important part hote hain. Ye switches generally core layer (ya backbone layer) mein use hote hain, jahan se large amount of data fast aur efficient tarike se flow hota hai.

Core Switches ke features:

1. High-Speed Data Transfer – Core switches high-speed connectivity provide karte hain, jo large-scale networks mein fast data transfer ensure karte hain.
2. Centralized Data Handling – Ye switches centralized point banate hain, jahan saare major network connections merge hote hain.
3. Scalability – Core switches network ko expand karne mein madad karte hain, jise future growth ke liye prepare kiya ja sakta hai.
4. Redundancy – Ye ensure karte hain ki network ki uptime rahe, aur agar ek route fail ho jaye to doosra path use ho sake.
5. High Bandwidth – Core switches ke paas zyada bandwidth hota hai, jo heavy data traffic ko efficiently handle kar sake.

Core Switch ka role in network:

* Central Hub: Ye main hub hote hain, jahan se data flow hota hai across all parts of the network.
* Connects Backbone Devices: Core switches backbone devices ko connect karte hain jaise data centers, routers, and other core network elements.
* Fast and Reliable: Inka kaam fast, reliable, aur error-free data transmission karna hota hai.

Example:

Agar aapka network ek city road system jaisa hai, to core switch wo main highway hoga jahan se sabhi traffic smoothly pass karte hain.

Popular Brands for Core Switches:

Cisco

Juniper

Arista

**• What is network management?**

* Network Management ka matlab hai network ke resources (jaise routers, switches, servers, cables, etc.) ko monitor, maintain, aur optimize karna. Iska main goal hai ki network efficiently aur securely kaam kare, aur problems ko jaldi solve kiya ja sake.

Network Management ke tasks:

1. Monitoring – Network ke performance aur health ko track karna (jaise speed, traffic, downtime).
2. Configuration Management – Network devices ko configure karna aur unki settings manage karna.
3. Fault Management – Network me jo issues aa rahe hain unhe detect karna aur solve karna (jaise device failure).
4. Security Management – Network ko secure rakhna, unauthorized access ko block karna, firewalls configure karna.
5. Performance Management – Network ki speed aur efficiency ko improve karna, bandwidth allocation manage karna.
6. Accounting/Usage Management – Network ka use kaise ho raha hai uska record rakhna, aur billing agar ho to manage karna.

Network Management Tools:

* SolarWinds
* PRTG Network Monitor
* Nagios
* Wireshark
* Cisco Prime

**• Explain Event Viewer**

* Event Viewer ek built-in tool hai Windows operating system mein jo logs aur events ko record karta hai. Ye tool system, application, aur security events ko track karta hai, jaise errors, warnings, aur information messages. Isse aap apne system ya network mein hone wali activities ko monitor kar sakte ho.

Event Viewer ke main features:

1. Log Events – Event Viewer system ke logs ko store karta hai, jo events ko record karte hain jaise software crashes, hardware issues, system errors, etc.
2. Filter Events – Aap specific events ko filter kar sakte ho jaise error, warning, information, etc.
3. Troubleshooting – Agar system mein koi problem ho rahi ho to aap Event Viewer ka use karke root cause pata kar sakte ho (jaise application crash ya system slowdown).
4. Security Monitoring – Login attempts, user activity, aur failed login attempts ko track kiya ja sakta hai.
5. Performance Monitoring – System ki performance ke baare mein detailed information milti hai, jaise memory usage, CPU load, etc.

Event Viewer ke sections:

1. Windows Logs:

* Application: Software-related events (errors, crashes).
* Security: Login attempts, access denials.
* System: Hardware aur OS issues.
* Setup: Installation aur configuration related events.

2. Custom Views – Aap custom logs bhi bana sakte ho specific events ke liye.

3. Applications and Services Logs – Specific applications aur services ke logs.

**• Practice "parental control" or "family safety" option in control pane What are network vulnerabilities?**

* Network Vulnerabilities wo weaknesses hain jo network security ko risk mein daalti hain, jiske through attackers ya unauthorized users aapke network ko breach kar sakte hain. Ye vulnerabilities aapke system ko hacking, malware, data theft, ya other security threats ke liye open bana deti hain.

Common Types of Network Vulnerabilities:

1. Unpatched Software – Agar network devices aur software updated nahi hain, to attackers inme existing bugs ka use kar sakte hain.
2. Weak Passwords – Simple ya default passwords network ko easily compromise karne ka mauka dete hain.

3. Open Ports – Agar unnecessary ports open hain to attackers ko entry mil sakti hai.

4. Unsecured Wireless Networks – Weak Wi-Fi encryption ya open networks (passwords nahi) easily hack ho sakte hain.

1. Social Engineering Attacks – Attackers users ko trick kar ke confidential information le lete hain (jaise phishing).
2. Malware – Malware ko system mein daal kar attackers sensitive information ya control access kar sakte hain.
3. Lack of Encryption – Agar network traffic ko encrypt nahi kiya gaya to attackers data intercept kar sakte hain.
4. Misconfigured Firewalls – Agar firewall sahi se configure nahi hai, to unauthorized traffic ko allow kiya ja sakta hai.

* Network Vulnerability ka example:

Maan lo ek company ka Wi-Fi unsecured hai aur koi unauthorized person is network ko access kar leta hai. Wo network par available sensitive data ko steal kar sakta hai, jo ek major vulnerability hai.

How to Fix Network Vulnerabilities:

1. Software and OS Updates – Regularly software aur devices ko update karo.
2. Strong Passwords – Strong passwords set karo, aur multi-factor authentication use karo.
3. Close Unnecessary Ports – Unused ports ko band kar do.
4. Wi-Fi Encryption – Wi-Fi network ko WPA3 ya WPA2 encryption se secure karo.
5. Use Firewalls – Properly configure firewalls aur access control list (ACLs) set karo.
6. Encryption – Sensitive data ko encrypt karo, taaki attackers usse read na kar sakein.
7. Regular Security Audits – Regular security audits aur vulnerability scanning karo.

**• What are the types of network security attacks?**

* 1: Malware Attacks
* Malware (Malicious Software) wo software hota hai jo network devices ya systems ko damage karta hai, data steal karta hai, ya control access le leta hai. Isme include hota hai:
* Viruses – Self-replicating programs jo systems ko infect karte hain.
* Worms – Standalone malware jo network par spread karte hain.
* Trojans – Software jo legitimate programs ke jaise dikhaate hain lekin hidden attacks karte hain.
* Ransomware – Malware jo files ko encrypt kar leta hai aur ransom maangta hai unhe decrypt karne ke liye.

2. Phishing Attacks

* Phishing ek social engineering attack hai jisme attacker fake emails ya websites banata hai jo genuine lagte hain, aur logon se sensitive information jaise passwords, bank details, ya personal info lene ki koshish karte hain.

3. Man-in-the-Middle (MITM) Attacks

* In attacks mein attacker user aur server ke beech mein aa jaata hai aur unka communication intercept karta hai. Yeh sensitive data jaise passwords aur credit card details ko steal kar sakta hai.

4. Denial-of-Service (DoS) Attacks

* DoS attack mein attacker kisi server ya network ko overload kar deta hai tak ki wo services dena band kar de. DDoS (Distributed Denial-of-Service) mein multiple systems se ek saath attack hota hai, jo aur bhi dangerous hota hai.

5. SQL Injection

* SQL Injection ek web application attack hai jisme attacker website ke database ko target karta hai aur malicious SQL commands send karta hai, jisse attacker sensitive data access kar sakta hai ya modify kar sakta hai.

6. Brute Force Attacks

* Brute Force attack mein attacker password ya encryption key ko guess karne ke liye har possible combination try karta hai. Iska goal hota hai unauthorized access lena.

7. Spoofing Attacks

* Spoofing mein attacker apne identity ko impersonate karta hai. Jaise:
* IP Spoofing – Fake IP address ka use karke network resources ko exploit karna.
* Email Spoofing – Email address ko fake karna taaki email genuine lage.
* DNS Spoofing – DNS responses ko manipulate karna taaki user incorrect websites par redirect ho jaye.

8. Cross-Site Scripting (XSS)

* XSS attack mein attacker malicious script ko web pages mein inject karta hai, jo users ke browsers mein execute hoti hai. Isse attacker sensitive information chura sakta hai.

9. Eavesdropping (Packet Sniffing)

* Eavesdropping mein attacker network ke through data packets ko intercept karta hai, aur sensitive information jaise login credentials, bank details, ya personal data steal kar sakta hai.

10. Zero-Day Attacks

* Zero-Day attack us waqt hota hai jab attacker kisi software ya system ke unknown vulnerability ka use karke attack karta hai. Yeh attacks us time par hote hain jab vulnerability ka patch release nahi hua hota.

11. Password Attacks

* Password Attacks mein attacker kisi system ke password ko crack karne ke liye methods use karta hai, jaise dictionary attacks aur rainbow table attacks.

12. Session Hijacking

* Session Hijacking mein attacker ek valid session token ko steal kar leta hai, jo usse authorized user ki tarah behave karne ka access deta hai.