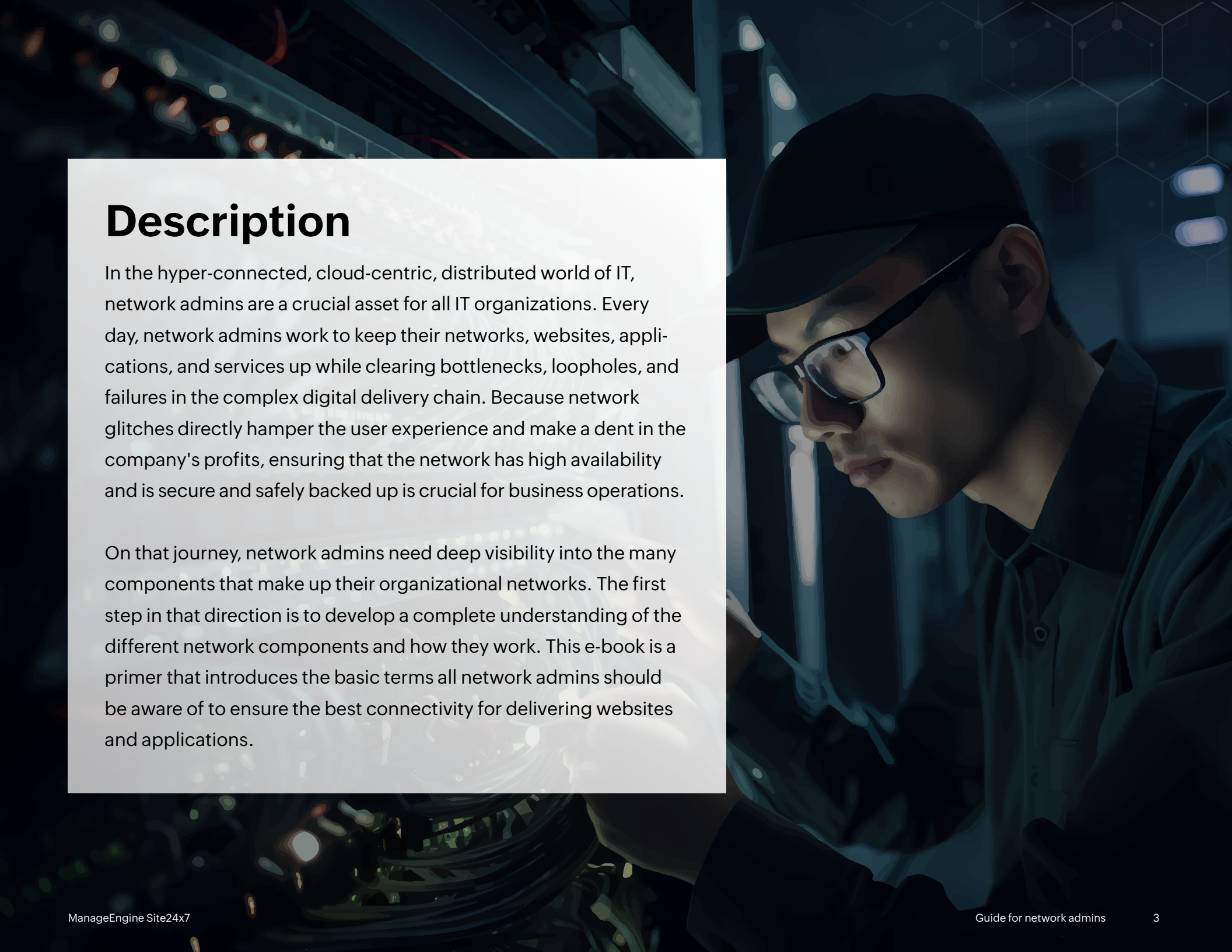
ManageEngine
Site24x7

Guide for network admins

What are we going to cover?



Description

In the hyper-connected, cloud-centric, distributed world of IT, network admins are a crucial asset for all IT organizations. Every day, network admins work to keep their networks, websites, applications, and services up while clearing bottlenecks, loopholes, and failures in the complex digital delivery chain. Because network glitches directly hamper the user experience and make a dent in the company's profits, ensuring that the network has high availability and is secure and safely backed up is crucial for business operations.

On that journey, network admins need deep visibility into the many components that make up their organizational networks. The first step in that direction is to develop a complete understanding of the different network components and how they work. This e-book is a primer that introduces the basic terms all network admins should be aware of to ensure the best connectivity for delivering websites and applications.

What is a network?

A computer network is formed by interconnecting two or more computers in different combinations to communicate and share resources. Computer networks run on a global standard called the Open Systems Interconnection (OSI) model. The internet is the world's largest interconnected computer network, exchanging data and enabling communication through interconnected networks with standardized communication protocols.

Who is a network admin?

A network admin is a specialist IT professional who configures, deploys, maintains, and monitors network infrastructures and services to ensure the best uptime, performance, and security. Network admins are also involved in the design stage of computer networks. A network admin configures switches, routers, virtual private network (VPN) gateways, and firewalls to secure their organization's IT infrastructure.

They also create and manage network security features, such as demilitarized zones (DMZs), and assign and control internal Internet Protocol (IP) addresses. Furthermore, they manage network services and protocols, such as Dynamic Host Configuration Protocol (DHCP), Domain Name System (DNS), File Transfer Protocol (FTP), HTTP, Network Time Protocol (NTP), and Network File System (NFS).

Network admins also make sure that their organizations always stay connected and secure by continuously monitoring their networks and testing them for weak links and breaches. Network admins are tasked with ensuring timely software updates, making backups of vital configurations, and enforcing all security protocols and access control lists (ACLs). Network admins are responsible for maintaining network security policies and standards, which involves communicating with all the stakeholders in their networks for awareness and adherence.

Networking fundamentals

Networking fundamentals begin with a study of the basic devices that make networking possible. A network is a logical, inclusive grouping of hosts that share the same IP address space and have similar connectivity needs. Networks can span from just two hosts (like in a home network) to millions of connected devices (like in a large organization). Enabled by service providers and governed by international protocols and laws, the internet is the ultimate network of interconnected networks.

What are hosts and clients?

Connected devices in a network are referred to as hosts. A client refers to either a computer or a computer program that seeks to access a server. Hosts send or receive data. Examples of hosts include computers, mobile phones, cloud services, and Internet of Things (IoT) devices. Hosts and clients (such as browsers) initiate requests, and servers (such as web servers) answer them.

What is a MAC address?

A media access control (MAC) address is a physical address burned into a computer device by the manufacturer. This permanent identifier is necessary for switches and other devices to route network packets.

What is an IP address?

An IP address is a unique identity for a host. The most widely used IP addresses are of type IPv4. IPv4 addresses are 32-bit, hierarchically assigned addresses. IP addresses enable hosts to connect with other hosts in a network without clashes.

What are the IP address versions?

IPs provide unique logical addressing schemes for computers to locate each other to communicate in an IP network. There are two major IP versions in vogue today: IPv4 and IPv6. IP addresses operate on the network layer of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol stack. IPv4 addresses are 32 bits in length and can hold a maximum of about four billion unique host addresses that can be identified on the internet. An IPv4 address has two parts to identify connected networks and specific devices: the network ID and the host ID.

There are also different classes of IPv4 addresses that vary according to which part of the IP address is allotted for the network ID and which part for the host ID. In a typical IP address such as 192.168.136.28, the 192 stands for 11000000, and so on, representing the binary bits in decimal numbers for brevity. IP addresses can be public (as identified on the internet) or private (meaning they are not connected to the internet or are behind firewalls).

What is TCP/IP?

TCP/IP is the standard communication protocol between networks. Two essential services run on TCP/IP: DHCP and DNS.

What is a network ID and host ID?

An IP address has two components: the network ID and the host ID. The first part, the network ID, points to the network segment that a host belongs to. The second part, the host ID, points to a specific network segment to communicate with other hosts within that segment directly at a faster rate of communication. There are five classes of IP addresses according to the different permutations of the network ID and host ID, with each of the five meant to be used for specific network types.

Why does IPv4 continue to be in use despite the introduction of IPv6?

Because IPv4 addresses were under threat of exhaustion in an ultra-connected future brimming with devices (such as IoT devices), the IPv6 standard with 128 bits of length was introduced. IPv6 accommodates a practically unlimited number of connections enough for the future (340 undecillion).

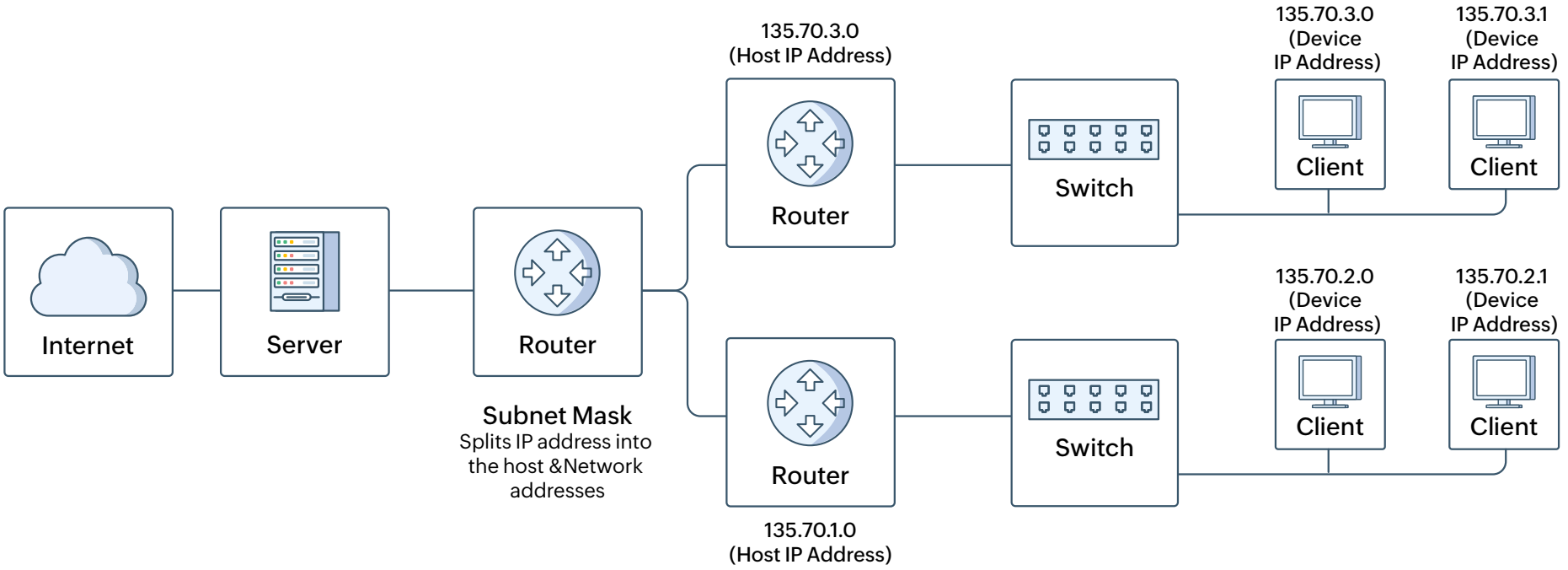
However, IPv4 has not vanished entirely, thanks to the concept of subnetting. That is why the adoption of IPv6 has not increased as expected and why IPv6 coexists with IPv4. An example of a valid IPv4 address is 192.0.3.126.

An example of a typical IPv6 address is 1234:0424:1CB3:0000:0000:0125:4565:24B5, with each digit being hexadecimal. The leading zeroes in an IPv6 address can be dropped, substituted for double colons, or reduced to single zeroes for brevity. For example, 1060:0000:0000:0000:0004:0500:100c:356c can be written as 1060:0:0:0:4:500:100c:356c.

IPv6 addresses have two parts: the network and the node. Furthermore, the network contains two subparts: the unicast address and the subnet ID. According to the types of network transmissions, IPv4 transmissions can be unicast (one-to-one), multicast (one-to-few), or broadcast (one-to-all). IPv6 transmissions can be unicast, multicast, or anycast (to the closest).

What is subnetting?

A subnetwork, or subnet, is a network within a network that shares a subnet configuration to



enable better connectivity through grouping. A subnet is a subset of a larger IP network. When you split a network into two or more subnets, computers within the same subnet can be referred to with only the most significant parts of their IP addresses, speeding up networks. Subnetting also makes reusable IPv4 addresses possible so that they are easily handled by the routers themselves.

What is Network Address Translation?

Network Address Translation (NAT) is a method of routing unroutable IP addresses statically or dynamically across public IPv4 addresses. This helps keep private IP addresses local. NAT hides the original, efficient, private IP addresses of devices behind firewalls to enable them to connect to the world outside.

What is the OSI model?

The OSI system is a global standard that describes seven standard layers that connect computers over a network.

These layers are as follows:

1. Physical
2. Data link
3. Network
4. Transport
5. Session
6. Presentation
7. Application

Layers 1 to 3 are hardware layers, and Layers 5 to 7 are software layers. Layer 4, the transport layer, is also referred to as the heart of the OSI model.

What are the types of networks?

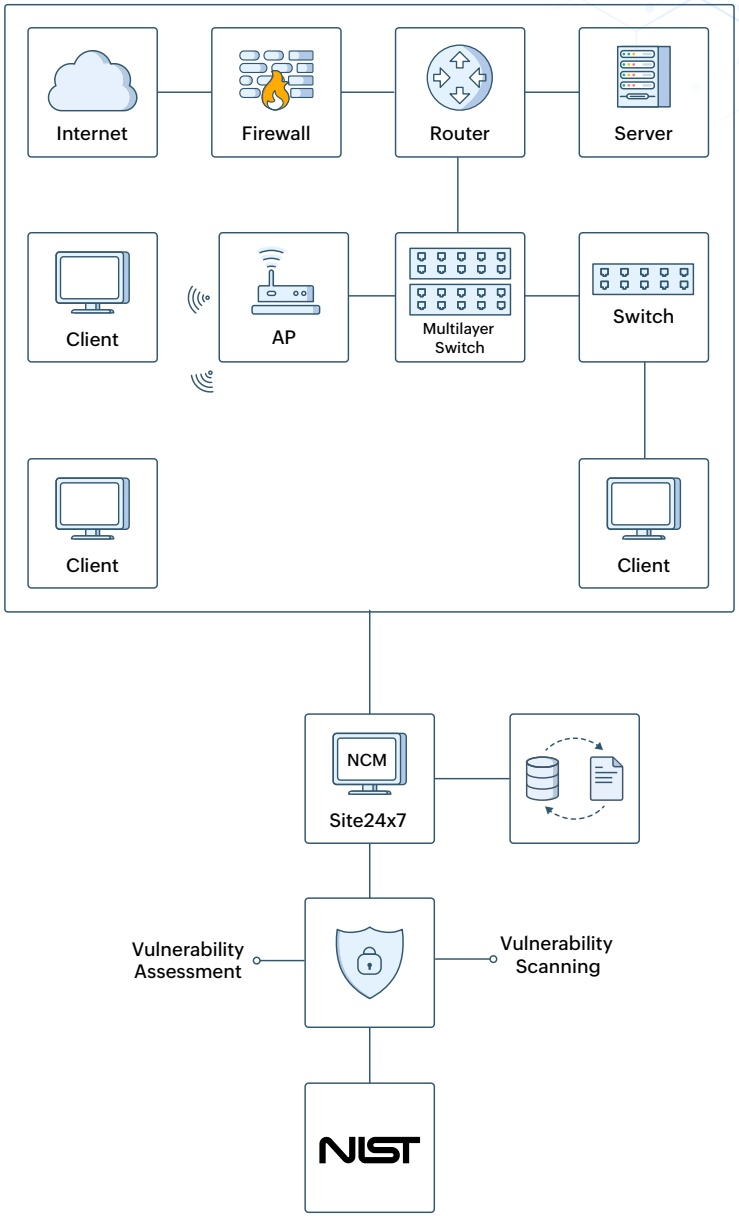
There are more than 10 types of computer networks, ranging from a couple of devices connected for printing documents to millions of devices in a global mesh working to fulfill a specific purpose.

The major types of networks are:

- Personal area networks (PANs): Enable small offices
- Local area networks (LANs): The simplest, most used type that connects devices in close geographical range
- Wireless LANs (WLANs): LANs connected without wires
- Metropolitan area networks (MANs): Typically the size of a town
- Wide area networks (WANs): Large networks, including the internet
- Storage area networks (SANs): Enable blazing-fast storage access
- VPNs: Provide secure, point-to-point networks for private connections
- Enterprise private networks (EPNs): Owned and operated by large companies
- Passive optical LANs (POLANs): An emerging, faster alternative to LANs

What are network topologies?

A network topology is the scheme in which network devices are connected to each other, determining the number of ways two devices can connect within the network. Network topologies are maps of networks that define their schemes and functions. Network topologies can be peer-to-peer, client- or server-based, or hybrid. Network topology models include the bus topology, ring topology, star topology, and mesh topology, according to how network signals traverse from one network node to another. Topologies can be either point-to-point or point-to-multipoint.



What are the types of network topologies?

- **Bus network:** Devices are joined by one cable like a pipeline. This is a simple, cheap, widely used type, but it's error-prone and less secure.
- **Ring network:** Each device connects to two others, making the whole network a circular loop or ring in shape. Ring networks are fast, but when one link falls, the whole network goes out of order.
- **Star network:** This is a ring network with an additional hub or switch acting as the center that connects to all the nodes of the network. Star networks are reliable and have redundancies but are expensive to install, maintain, and troubleshoot.

What are the types of network communication devices?

- **Repeaters:** Layer 1 devices that amplify signals to enable long-distance communications
- **Hubs:** Devices that act as multi-port repeaters that duplicate requests, broadcast, and stream data between hosts in a network
- **Bridges:** Devices that connect hubs and restrict data exchanges to authorized devices only
- **Switches:** Layer 2 devices that transfer data between MAC addresses
- **Routers:** Traffic regulator devices that connect networks, have IP addresses called gateways to transfer data between networks, and hold routing tables to remember data pathways
- **Other network devices:** Access points, load balancers, firewalls, intrusion detection systems (IDSs) and intrusion prevention systems (IPSs), proxies, virtual switches and routers, and Layer 3 switches that fulfill a variety of communication needs

What is routing?

Routing is the process of deciding the optimal path for delivering a data packet between networks. A Layer 3 device performs this process, bridging different methods to enable communication.

Static routing involves routes defined by network admins for small networks. Dynamic routing uses dynamic protocols to enable complex connections, making the internet possible. While admins define default routes to mark the next hop for data packets, a routing table is an automated table dynamically built to mark all known routes from the router's perspective to enable efficient connections.

Routing tables help with route aggregation by summarizing routes to different networks through the Classless Inter-Domain Routing (CIDR) protocol, also called supernetting. Route aggregation is a method used by network admins to optimize routing tables to make them efficient by summarizing them using CIDR. In routing, the next hop is the next router along the way, a routing table is a database table that finds the best possible network route, and convergence is the time taken for all routers within an autonomous system (AS) to learn all the possible routes within it.

What are the key routing metrics?

- **Hop count:** The number of routes between two endpoints from a sending router's perspective
- **Maximum transmission unit (MTU):** The data packet size
- **Bandwidth:** The speed of a network connection in megabits per second or gigabits per second
- **Latency:** The time it takes for a packet to traverse a route and reach its destination
- **Administrative distance (AD):** The believability of an advertised route's ability to send packets (the lesser the AD, the more believable)

What are the routing protocols?

There are interior gateway protocols (IGPs), such as Open Shortest Path First (OSPF), that are used within ASs. There are also exterior gateway protocols (EGPs), such as Border Gateway Protocol (BGP), that are used between ASs. Routing protocols are also classified according to the method of determining the routes: distance-vector routing protocols, path-vector protocols (like BGP), link-state protocols, and hybrid routing protocols.

What is Multiprotocol Label Switching?

Multiprotocol Label Switching (MPLS) routes traffic through the shortest path identified by labels. MPLS enables higher speeds and better security by streamlining data through labeled paths while avoiding lookups into routing tables. Instead of routing packets about each hop with source and destination addresses, MPLS routes with predetermined labels so packets hit the destination faster, like an express courier service, and is thus costly.

What are Autonomous Systems?

An AS is a large group of networks that collectively follow a common routing policy. Universally, these ASs are assigned unique 16-bit autonomous system numbers (ASNs) that act as zip codes interconnecting with each other to form the internet. Internet service providers (ISPs), large organizations, and governmental bodies operate ASs around the world. Each AS is assigned a set of IP address spaces to attach to the devices within.

What is BGP?

BGP is a gateway protocol that helps internet devices with peering and exchanging routing information between ASs. BGP is also called the routing protocol of the internet as it routes data packets between ASs, which announce their routing information to BGP. BGP uses these announcements to construct and update routing tables, enabling communication across the internet.

What is software-defined networking?

Software-defined networking (SDN) is dynamically administering and configuring a network using a front-end program. SDN allows network admins to adjust network performance in a centralized, efficient, continuous manner. SDN is quickly gaining traction as MPLS use has been declining since 2019.

What are VPNs?

VPNs are used for remote hosts and sites to communicate privately using protocols such as IPsec, ISAKMP, Transport Layer Security (TLS), and Secure Sockets Layer (SSL). VPN data travels through encrypted tunnels via a public network securely and cost-effectively.

What are network security devices?

Firewalls police IT networks. Firewalls are software or physical devices that inspect every packet to determine whether or not to allow it across a network barrier, ensuring a secure connection. IDSs are passive systems that alert the network admin to breaches or attacks. IPSs are active systems that guard a network to block any offending IP addresses and terminate network sessions during breaches.

What are network and performance optimization devices?

Load balancers, also called content switches or filters, help even out uneven workloads to achieve significant efficiency and speed. A proxy server is a device that covers your client identities when contacting external servers and also filters and caches content.

What are network authentication services?

Network devices such as network interface controllers (NICs) are physical cards that connect devices to a network. Network access service protocols include Remote Authentication Dial-In User Service (RADIUS) and Terminal Access Controller Access-Control System Plus (TACACS+), which enable secure remote access.

Network admins should also know the basics of special network services, such as remote access services (RASs), XML communications, and unified voice services that help integrate voice channels into a network.

To safeguard network connections, there are further standards in secure information transport: SSL and its more secure and latest avatar, TLS. SSL and TLS connections over HTTP are accompanied by a padlock symbol to establish authenticity.

What is DHCP?

DHCP is the system that automatically (dynamically) configures and assigns IP addresses for every network host, saving network admins from configuration work. All network servers and many routers come with built-in DHCP server functions. While small networks can have static IP addresses micromanaged by network admins, big networks are more prone to complexities and errors and thus demand automation.

DHCP solves scaling issues by automating the IP configuration process and making it easy to update and maintain default gateways. Network admins also configure critical DHCP parameters (such as the lease window, which specifies for how long a connection is valid) and set preferred IP configurations whenever needed.

Some concepts associated with DHCP

- **Static IP address:** This is an unchanging, permanent IP address that is used when there is a need for multiple external devices or services to establish contact with the host, such as a VPN or printer in a large network.
- **Leased IP address:** This is a temporary IP address assigned by a DHCP server to a host.
- **Subnet mask:** This is a technique that helps hosts know which network they are on.
- **Gateway address:** This is the ISP that further connects hosts to the internet.
- **Assigning IP addresses to machines:** A new node in a network usually broadcasts a discover message, to which the DHCP server replies with an offer message. Upon receipt of the offer, the host broadcasts a DHCP request message, which is then assigned network information, which is valid until the host detaches itself by sending a release request.

What is DNS?

Called the internet's phone book, DNS helps humans connect to web resources through easy-to-identify names rather than actual IP addresses. At its core, DNS is an iterative, multilayered system that passes requests through layers of specific servers that zero in on specific IP addresses to enable browsers to connect.

For example, "www" is the internet, "google" is the local domain, and ".com" is the top-level domain (TLD) that locates the specific webpage of www.google.com. Network admins should also configure local DNS servers that maintain a cache of IP addresses in the local subdomain to save time.

DNS works through TCP/IP to assign unique, easy-to-remember names instead of mere numbers to point to host systems. DNS follows a clearly-defined hierarchical system of naming conventions that involves recursive servers that point to root servers as well as authoritative servers that store and serve IP addresses linked to unique DNS names, making the internet easy to navigate. There can also be subdomains within DNS, which can be assigned for specific purposes. Network admins must be aware of how DNS servers maintain DNS records and the basics of how dynamic DNS works.

How DNS resolves a website's actual IP address to enable a browser to connect with itStatic IP address:

- The user requests www.demonstration.com. The browser checks the DNS cache for the site and connects directly if it is found. Otherwise, the browser reaches out to the DNS resolver hosted by your ISP.
- The ISP asks the root name server (RNS), which returns the TLD for the ".com" domain.
- The resolver contacts the TLD server, which returns the location of the authoritative name server (ANS) that holds the IP addresses of websites within the ".com" domain.

- Now, the resolver reaches out to the final authority: the ANS. The ANS returns the IP address of the web server for www.demonstration.com.
- The browser now connects, downloads the website content, and stores the address in its local cache to load it faster next time.

What are the types of network connections?

Network admins should be aware of the history of network transmissions, including the public switched telephone network (PSTN), dial-up modems, Integrated Services Digital Network (ISDN), digital subscriber line (DSL), coaxial cable networks, fiber-optic networks, broadband, LANs, WANs (circuit-switched networks, packet-switched networks, and MPLS), and leased line networks.

Knowledge about wireless technologies such as Wi-Fi networks and cellular networks, like GSM, CDMA, HSPA+, LTE, and 5G, is essential. Network admins should also know the basics of coaxial cables, fiber-optic cables, twisted-pair network cabling (RJ11, RJ45, RJ48C, etc.), couplers, media converters, connectors, and cabling tools that enable connectivity.

What are the different types of network implementations?

Network infrastructure can be implemented through various schemes that include LANs, MANs, and WANs (including the internet). There are also PANs that exist between personal devices. Furthermore, there are special use network configurations, such as supervisory control and data acquisition (SCADA) and Cisco Medianet, that enable low latency and rich voice and video transmissions.

A 20-point checklist for network admins to achieve the best uptime and security for their network IT assets

1. Eliminate single points of failure

Ensure that networks are up and active for the maximum amount of time by proactively spotting and eliminating single points of failure. Install additional safeguards to prevent disastrous consequences from unchecked actions, like a sudden reboot of a file server. One high availability technique is to ensure redundant networks and backup protocols that operate outside your subnets for you to fall back on whenever the main networks go out of order.

Plan your routing tables well and revise them often to avoid large, cumbersome tables. Work to eliminate weak links that could potentially take entire networks off the grid. Ensure redundant links to outside networks through techniques like Hot Standby Router Protocol (HSRP) and Virtual Router Redundancy Protocol (VRRP). These are ways to ensure high availability and avoid single points of failure in networks.

2. Open communication channels

More importantly, when networks go down, ensure that you instantly relay sufficient information to your customers who depend on your products and services. Enabling a third-party, independently hosted status information page like StatusIQ is a great way to keep your users informed about outages, including planned ones, to ensure brand trust.

3. Adopt a solid backup plan

Having a bulletproof backup plan is indispensable for network continuity. Think with a guardian mentality because any action you take as a network admin will have a cascading effect on multiple users. Always maintain well-indexed file systems with back-ups that are easy to retrieve and restore. When a network file needs to be updated, don't copy it to a local drive to update it in isolation as a clash during replacing it may put your network into disarray.

After setting up your backup plan, ensure that the procedures are adhered to by conducting surprise checks. Ensure that the most critical files have two backups and are safely stored.

4. Draft a network management questionnaire

Have an elaborate network management questionnaire that includes questions such as:

- What are the network layers to monitor?
- Are third-party performant and available systems (like content delivery networks (CDNs) and the DNS) and the protocols they depend on (like TCP and BGP) functional?
- Are my DNS queries getting resolved?
- Can we zero in on any issue across our DNS resolution chain?
- Is my DNS resilient to attacks, and does it have service integrity?
- Is my CDN functioning optimally?
- Is BGP secure from these vantage points?
- What are my remote troubleshooting abilities?
- How do I optimize the user experience by ensuring adequate interconnections?
- Is my wireless network (and its critical paths) healthy and observable?
- Is Secure Shell (SSH) configurable with the intended server?
- Can I receive SMTP and IMAP emails as expected?
- Is FTP functioning both ways to upload and download files?
- Is NTP in sync to ensure the error-free functioning of interconnected networks?
- Are all third-party components beyond my control reachable and observable, such as APIs that connect different applications?
- Do I have functional dashboards that pool the data from various observable network components to provide actionable insights whenever and wherever?

Ensuring that all these questions are taken care of will directly correlate to a smooth user experience for your end users.

5. Ensure all technical precautions

Make sure your networks are always guarded. Set wireless access points carefully, ensuring maximum security with strict controls. Have good password hygiene and complete awareness of the network and permitted devices. Hiding the service set identifier (SSID), disabling guest modes, checking rogue access points, ensuring prompt security patches and virus protection, enabling backup points and firewalls, and enforcing MAC address filtering are some of the best practices for safeguarding your wireless networks.

6. Implement network policies systematically

Before you even install your network server, draft a plan for TCP/IP settings that includes the IP subnet address, a domain name for your network, a static IP and host name for your server, default gateways, and clarity on DHCP and DNS use. Have a contingency plan and a ready reckoner of all the critical commands and protocols handy to help you during emergencies such as breaches or network breakdowns. Document and validate your scripts with peers. Simulate your changes whenever possible, include detailed configuration snippets and dates, and version control your scripts.

7. Take proactive measures

Use intelligent forecasting methods to ensure you don't run out of network server space. A shortage of a few gigabytes on your server may make your computers crawl and errors pop up in large numbers. This goes hand in hand with good digital housekeeping, which involves removing unwanted files, such as outdated logs. Make proper backups of your network configurations. Use an industry-standard network configuration manager to help you systematize your network management routines.

8. Be emergency ready always

Establish a response system for your help desk and escalation matrix and constantly be on your guard. There are no days off or lean days for network management for as long as your business functions. Have backup personnel ready and fully trained to handle mission-critical activities in network management. Have the proper communication channels to contact your user base whenever needed. Hosted status pages help reduce the number of tickets during outages and strengthen brand trust by ensuring transparent, straightforward communication about the state of your network. More importantly, document all your network events and make the documentation accessible for your team to deal with crises.

9. Define your network needs

List your desired network features and the budget available to set them up. List the equipment and shared resources needed and plan for future scaling needs. Decide whether your clients will receive their IP addresses statically or through a DHCP server. Also, plan your firewall strategy and set up a DMZ that protects the internal network from undesired outside exposure.

For wireless configurations, network admins have to set an SSID name and enable encryption to secure communications. Employ active network monitoring techniques, including using port scanners that scan open ports and protocols within a network to ensure uptime and spot vulnerabilities. Packet flow monitoring helps network flow identify top routes, and Wi-Fi analyzers analyze wireless network activity.

10. Document your network configurations

Network configuration management is the practice of evaluating, managing, documenting, gatekeeping, and changing an IT network. Any changes to your network configurations should be systematically recorded in a centralized database as backups. Use third-party network configuration managers such as Site24x7 to record your changes and restore your network to a previous, functional state during breakdowns.

11. Record your network baselines

Network admins should document the ideal network states as log files to establish good network performance. This way, any deviations in metrics, such as CPU usage and bandwidth usage, can be spotted and corrected to base levels.

12. Track key network metrics

To know your network's health, you must keep track of its key metrics constantly and log all events systematically. Set intelligent alerts to be in the know when network issues happen. Use Simple Network Management Protocol (SNMP) to monitor and manage your network and set up traps that spot anomalies and trigger real-time alerts.

13. Use connectivity utilities

Ping is a method of echoing requests between nodes to check if the connection is functional. Traceroute is a utility that determines the path data takes between two nodes in a network. Microsoft offers a combination of the above methods, pathping, which establishes a ping test on each data hop between two nodes. Tools like ipconfig, Address Resolution Protocol (ARP), and nslookup help troubleshoot connectivity issues.

14. Follow network hardening techniques

Ensure that the latest version of SNMP is used to ensure secure connections. Whenever possible, use SSH connections over Telnet for connecting remotely to devices during troubleshooting. Also, choose Secure File Transfer Protocol (SFTP) instead of the unsecure FTP to transfer files. Choose TLS to authenticate security keys, HTTPS for secure web browser connections, and IPsec to secure all data transmissions.

15. Master good log management

Don't drown in a large dump of unseparated, haphazard log files. Compare logs against the baseline documentation, archive them systematically, and identify the key network metrics that must be consistently recorded with your log management tool. Use security information and event management (SIEM) tools to analyze long-term log data and proactively tweak your network to suit your emerging needs.

16. Strengthen your network policies

To track and upgrade your assets, create and periodically update network policies and procedures, including network asset documentation. Also, maintain physical maps of your network devices and connections along with logical network diagrams to detail all the assets in your network. Maintain robust vendor documentation to keep track of license contracts and service-level agreements (SLAs) concerning your network.

Ensure clarity in workgroup access policies and centralize software management for all devices within the network. Have a particular mobile device policy and work-from-home guidelines with zero room for ambiguity. Use group policies to control your Active Directory environment and clarify network access restrictions and guidelines.

Establish an email and file transfer policy that includes Sender Policy Framework (SPF), blocklisting, graylisting, allowlisting, and keyword filtering. Restrict all outside access to your network and disallow unrestricted access to untrustworthy domains at the system level. Cleaning up the network server by removing unwanted, outdated configuration files and backups that clog your systems is also essential for the best upkeep of your network. T

17. Clarify your BYOD policies

Implement network admission control policies for employee-owned devices that connect to your company's IT systems from various network access points. Clear BYOD policies help set expectations and restrictions to safeguard your network devices from vulnerabilities while ensuring prompt security and software updates. Enable antivirus and antimalware programs for all connected devices. Make sure that user authentication is secure by using multi-factor authentication and single sign-on.

18. Eliminate errors by design

Use fail-safe systems (poka-yokes) that prevent network shutdowns during critical updates to avoid losing critical data. Never assume anything and always double-check network configurations, backups, and disaster management drills. Wherever possible, automate to eliminate errors by design.

19. Create a business continuity plan

Network admins should create, maintain, and periodically update a business continuity plan (BCP) with a complete disaster recovery playbook. The plan should put safety first and list ways to secure all the components in the network, with priorities for fallback processes and recovering critical systems.

20. Enforce the Zero Trust model

Never leave network access settings unguarded. All users at all levels must verify themselves to access a resource. The access lists of approved users should be updated periodically to eliminate old accounts. Also, follow best practices in managing your daily work as a network administrator. Never write passwords on paper, never compromise on software, and always automate patches and updates so as not to leave room for manual errors. Use password generators, two-factor authentication, and physical keys to block access to network installations. Stay guarded out of sheer habit.

Conclusion

A network admin's job is an ever-evolving one that requires constant learning because technological changes are faster in networking. This 20-point checklist will especially help new network admins plan out robust work strategies to run and maintain their IT networks to benefit their businesses globally.

About ManageEngine Site24x7

Site24x7 offers AI-powered full stack monitoring for DevOps and IT operations with telemetry data collected from servers, containers, networks, cloud, database, applications and provide AI-powered full stack observability. Additionally, Site24x7 can track end user experience via synthetic and real user monitoring capabilities. DevOps & IT teams can use these capabilities to troubleshoot and resolve application downtime and performance issues, infrastructure issues and better manage the digital user experience. For more information on Site24x7, please visit **www.Site24x7.com |**

Email: eval@site24x7.com

Get Quote | Request Demo