Network Administrator

Written by [Febogamedev]

After examining how networks are structured and how devices communicate with one another, we can introduce a very important professional role: t**he network administrator**.

A network administrator is responsible for designing, configuring, monitoring, and maintaining a computer network (U.S. Bureau of Labor Statistics, 2023).
Their main responsibility is to ensure that computers, servers, printers, access points, switches, routers, and other devices can communicate correctly with one another and, when necessary, with the Internet (U.S. Bureau of Labor Statistics, 2023).

In a school, company, or office, the network administrator is primarily responsible for the structure of the local network.
For example, they decide how to connect the various devices, where to place switches, how to configure Wi-Fi access points, and how to organize the different areas of the network.

One of the network administrator's main tasks is configuring network equipment U.S. Bureau of Labor Statistics, 2023).
This equipment may include routers, switches, firewalls, access points, and servers.
Each device must be configured correctly to perform its function:

- The switch must connect the devices within the LAN.
- The router must route packets between different networks (Baker, 1995).
- The firewall must enforce security rules (Scarfone & Hoffman, 2009).
- The access point must allow wireless devices to connect to the network.

The network administrator is also responsible for network addressing.
Every connected device must have the information required to communicate (Droms, 1997).

Another important task is managing users and permissions.
In a school or company network, not everyone should have access to the same resources. For example, students might have access to the Internet and certain shared folders, while teachers or administrative staff might have access to different services. The network administrator must therefore configure accounts, groups, permissions, and access policies (Joint Task Force, 2020).

Security is a fundamental part of the job.
The administrator must protect the network from unauthorized access, malware, incorrect configurations, and risky behavior (Pascoe et al., 2024).
For this purpose, they may configure firewalls, strong passwords, secure Wi-Fi networks, system updates, backups, antivirus software, monitoring systems, and rules that restrict access to specific services (Joint Task Force, 2020; Scarfone & Hoffman, 2009; Souppaya & Scarfone, 2022).

A network administrator must also monitor the operation of the network (Dempsey et al., 2011).

This means checking whether devices are reachable, whether the Internet connection is working, whether there are slowdowns, whether a server is unresponsive, or whether an access point has too many connected devices.
Monitoring helps identify problems before they become serious and allows the administrator to respond quickly when something stops working (Dempsey et al., 2011).

When a problem occurs, the network administrator performs troubleshooting, which involves diagnosing and resolving faults (Nelson et al., 2025).
For example, if a computer cannot access the Internet, the administrator must determine whether the problem involves the computer, cable, switch, Wi-Fi connection, router, firewall, ISP connection, or something else.
Solving a network problem therefore requires following a logical procedure and checking one component at a time.

The network administrator is also responsible for maintenance.
This includes updating software and firmware, replacing faulty equipment, documenting configurations, checking backups, evaluating performance, and planning possible network expansions (Souppaya & Scarfone, 2022).
A network is not something that is configured only once: it must be monitored and updated over time (Pascoe et al., 2024).

In some organizations, the network administrator is also responsible for dividing the network into separate areas.
For example, in a school it may be useful to separate the students' network from the teachers' network, the administrative offices' network from the guest network, or the laboratory network from the server network.
This separation improves organization, security, and traffic control (Joint Task Force, 2020; Scarfone & Hoffman, 2009).

The work of a network administrator therefore requires both technical expertise and organizational skills (U.S. Bureau of Labor Statistics, 2023).
Knowing how to connect cables or configure a router is not enough: the administrator must also document decisions, prevent problems, communicate with users, and find solutions suited to the specific context (Pascoe et al., 2024; U.S. Bureau of Labor Statistics, 2023).

Supplementary materials

Key points

- **The network administrator** designs, configures, monitors, and maintains a computer network.
- They configure devices such as **switches**, **routers**, **firewalls**, **access points**, and **servers**.
- They manage **network addresses**, user accounts, groups, and permissions.
- They protect the network through firewalls, passwords, updates, backups, and monitoring systems.
- They monitor performance, connections, and device operation.
- They perform **troubleshooting** by identifying and resolving faults through a step-by-step checking process.
- They may divide the network into separate areas to improve security and organization.
- Their work requires technical and organizational skills, as well as the ability to communicate with users.

Exercises

Designing a School Network

A school opens a new building consisting of:

- Two computer laboratories.
- A staff room.
- Several administrative offices.
- A Wi-Fi network for students.
- A Wi-Fi network for guests.
- A server containing confidential documents.

You are the network administrator responsible for organizing the new infrastructure.

- Identify which network devices may be needed among switches, routers, firewalls, access points, and servers.
- Explain the function each device would perform within the network.
- Propose how you would separate the different areas of the network, indicating which groups of users should be allowed to access the various resources.
- Explain why students should not necessarily have the same permissions as administrative staff.
- Identify some security rules you would configure to protect the network.
- Explain why the administrator should document the network structure and the configurations that have been implemented.
- Identify at least three activities that should be carried out periodically even after the network has been installed.

The Computer Cannot Access the Internet

A teacher reports that their computer can no longer access the Internet.

The other computers in the same classroom are working normally, and the school server can still be reached from the rest of the network.
The administrator must identify the problem without randomly replacing components.

Describe a troubleshooting procedure.

- Identify which elements you would check first on the teacher's computer.
- Explain why it is useful to check one element at a time instead of changing several configurations at once.
- If the computer uses a network cable, explain how you could verify whether the problem concerns the physical connection.
- If the local connection works but the Internet is still unreachable, identify which other network elements could be checked.
- Explain why, given that the other computers are working, some possible causes become less likely.
- Imagine instead that suddenly no computer in the school can access the Internet. Explain how your diagnosis would change and which devices or services you would check first.
- Explain how a monitoring system could help the administrator identify the problem more quickly.

Protecting and Maintaining the Network
The administrator of a small company discovers the following situations:

- All employees use the same password to access a shared folder.
- Some computers have not received updates for many months.
- Backups are performed, but nobody checks whether they can actually be restored.
- One access point is constantly overloaded.
- Some former employees still have active accounts.
- Nobody has documented the changes made to the network during the past year.

Analyze the situation.

- For each problem, identify which network administration activity has been neglected.
- Propose a concrete solution for each problem.
- Explain why keeping accounts that are no longer needed represents a security risk.
- Explain why installing software and firmware updates is part of both network maintenance and security.
- Explain why performing backups is not sufficient if they are never tested.
- Indicate how monitoring could help identify the overloaded access point problem.
- Propose a simple periodic maintenance plan, indicating which checks you would perform every week, every month, and whenever the network is modified.
- Explain why the work of a network administrator is not limited to "fixing the network when it breaks," but also includes prevention, organization, and planning.

Bibliography

Baker, F. (Ed.). (1995). *Requirements for IP version 4 routers* (RFC 1812). RFC Editor. https://doi.org/10.17487/RFC1812

Dempsey, K., Chawla, N., Johnson, L., Johnston, R., Jones, A. C., Orebaugh, A., Scholl, M., & Stine, K. (2011). *Information security continuous monitoring (ISCM) for federal information systems and organizations* (NIST Special Publication 800-137). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-137

Droms, R. (1997). *Dynamic Host Configuration Protocol* (RFC 2131). RFC Editor. https://doi.org/10.17487/RFC2131

Joint Task Force. (2020). *Security and privacy controls for information systems and organizations* (NIST Special Publication 800-53 Rev. 5). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-53r5

Nelson, A., Rekhi, S., Scarfone, K., & Souppaya, M. (2025). *Incident response recommendations and considerations for cybersecurity risk management: A CSF 2.0 community profile* (NIST Special Publication 800-61 Rev. 3). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-61r3

Pascoe, C., Quinn, S., & Scarfone, K. (2024). *The NIST Cybersecurity Framework (CSF) 2.0* (NIST Cybersecurity White Paper 29). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.29

Scarfone, K., & Hoffman, P. (2009). *Guidelines on firewalls and firewall policy* (NIST Special Publication 800-41 Rev. 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-41r1

Souppaya, M., & Scarfone, K. (2022). *Guide to enterprise patch management planning: Preventive maintenance for technology* (NIST Special Publication 800-40 Rev. 4). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-40r4

U.S. Bureau of Labor Statistics. (2023). *Network and computer systems administrators*. https://www.bls.gov/oes/2023/may/oes151244.htm

Further reading

- Jill West, CompTIA Network+ Guide to Networks, 10th ed., Cengage, 2025 — Provides a practical introduction to network administration, including network design, hardware configuration, addressing, wireless networks, security, monitoring, maintenance, and systematic troubleshooting of common network problems.
- Anthony J. Sequeira, CompTIA Network+ N10-009 Cert Guide, 2nd ed., Pearson IT Certification, 2025 — Covers the main technologies a network administrator works with, including routers, switches, firewalls, access points, addressing, network services, security, monitoring, troubleshooting, and modern network infrastructure.
- Wendell Odom, David Hucaby, and Jason Gooley, CCNA 200-301 Official Cert Guide Library, 2nd ed., Cisco Press, 2024 — Offers a more technical and hands-on approach to configuring and troubleshooting switches, routers, IP networks, wireless networks, access control, security mechanisms, and other technologies commonly managed by network administrators.
- Thomas A. Limoncelli, Christina J. Hogan, and Strata R. Chalup, The Practice of System and Network Administration: DevOps and Other Best Practices for Enterprise IT, Volume 1, 3rd ed., Addison-Wesley Professional, 2017 — Focuses on the professional and organizational side of administration, including infrastructure management, documentation, automation, maintenance, change management,

reliability, communication with users, and practices for operating IT systems over time.
- Chris Sanders, Practical Packet Analysis: Using Wireshark to Solve Real-World Network Problems, 3rd ed., No Starch Press, 2017 — Provides a practical introduction to network monitoring and troubleshooting through packet analysis, showing how to diagnose connectivity problems, DNS failures, slow networks, suspicious traffic, and other issues that network administrators encounter in real environments.

Editorial notes

In producing these materials, I have used generative artificial intelligence tools to support the writing process, particularly to improve the form of the text, reorganize content, refine wording, and speed up certain editorial tasks.

As I work independently on the production of these materials, I try to automate any activities that can reasonably be automated, so that I can devote more time to research, design, and content development.

However, artificial intelligence does not determine the content of this work: the choice of topics, structure, ideas, interpretations, examples, and teaching approach are developed by me. AI is therefore used primarily as a tool to support production and formal revision, while authorship and responsibility for the design and content remain mine.