Share on your Social Media

CCNA Tutorial

Published On: August 2, 2024

CCNA Tutorial

An IT certification for networking entry-level is the Cisco Certified Network Associate. Go through this CCNA tutorial to learn the basics of the field that equip you to enter networking jobs.

Download CCNA Tutorial PDF

Introduction to CCNA

Cisco Systems offers a well-liked networking certification program called CCNA (Cisco Certified Network Associate). The purpose of the CCNA certification is to assess a candidate's knowledge and abilities related to the installation, configuration, operation, and troubleshooting of medium-sized business branch networks.

This CCNA tutorial covers the following:

Related Course at SLA

Related Posts

Tableau Developer Salary in Chennai

Published On: October 12, 2024

Introduction A Tableau Developer designs, develops, and maintains dashboards and visualizations using Tableau software. Key...

- Overview of CCNA
- Installing, configuring, and maintaining networks.
- Advanced troubleshooting techniques
- Understanding of automation and security.

CCNA Interview Questions

Overview of CCNA

The CCNA certification covers many topics, including network automation, infrastructure, security, and networking fundamentals.

- Configuring, understanding, using, and troubleshooting switched and routed networks.
- It assists users in establishing a point-to-point connection.
- The CCNA provides instructions and examples for creating a network address.
- If you study at CCNA, you'll land a well-paying job.

What is a network?

A network comprises two or more separate computers or devices connected to exchange files, share resources (such as printers and CDs), or enable electronic interactions.

The most common types of networks are as follows:

Personal Area Network (PAN)

This is a computer network centered on an individual. A computer, mobile device, or personal digital assistant is typically part of it.

These portable gadgets can communicate with one another over a PAN to connect to the internet and a digital network.

Local Area Network (LAN)

A collection of connected computers and

VMware Tutorial for Cloud Computing Aspirants
Published On: October 12, 2024

VMware Tutorial for Cloud Computing Aspirants VMware software allows you to run a virtual machine...

VBA Macros Tutorial for Beginners
Published On: October 10, 2024

VBA Macros Tutorial for Beginners VBA macros are programs that automate repetitive operations in Microsoft...

VB.Net Tutorial for Beginners
Published On: October 10, 2024

VB.Net Tutorial for Beginners Visual Basic is an easy-to-learn programming language that is type-safe. Get...

peripherals in a small space, such as a home, office building, lab, or school, is called a local area network, or LAN.

LAN is used for sharing resources like files, printers, games, and other applications.

Wide Area Network (WAN)

A WAN network system can be a local area network (LAN) that uses radio waves and phone lines to connect to other LANs. It is primarily restricted to a business or organization.

Metropolitan Area Network (MAN)

A computer network spanning a whole city, a college campus, or a small area is called a metropolitan area network, or MAN. Compared to a LAN, which is typically restricted to a single building or location, this kind of network is larger.

With this kind of network, you may cover a range of several miles to tens of miles, depending on the setup.

CCNA Salary

Internetworking Devices in Network

We need a variety of internet-working devices to connect to the internet. Several gadgets are frequently utilized in the process of establishing the Internet.

- **NIC: Network Interface Card:** Workstations are equipped with printed circuit boards. It symbolizes the physical link that exists between the network cable and the workstation.
- **Hubs:** By amplifying and retransmitting the signal, a hub helps a network cabling system go farther.
- **Bridges:** They are frequently split up into smaller LANs to manage the bigger network.

Bridges are used to connect these smaller LANS.

- **Switches:** With the help of switches, every workstation on the network can send data without affecting the other workstations.
- **Routers:** Data is sent to the destination device via the most cost-effective and efficient path possible with the help of a router.
- **Brouters:** They are an amalgam of a router and a bridge. Brouter functions as a filter, allowing some data to enter the local network while diverting unauthorized data to an external network.
- **Modems:** Modems are devices that change computer-generated digital signals into analog signals that can be sent over phone lines.

TCP/IP Layers

The **Transmission Control Protocol/Internet Protocol** is referred to as TCP/IP. It chooses the best way to connect a computer to the Internet and the best way to transfer data back and forth between them.

TCP: Data must be divided into smaller packets and sent over the network.

IP: It manages the addressing, sending, and receiving of data packets across the internet.

Network Segmentation

Segmenting a network entails dividing it up into smaller networks. It facilitates the division of traffic loads and increases Internet speed.

The following methods can be used to create network segmentation:

- By putting in place gateways and DMZs (demilitarized zones) between networks or systems with various levels of protection.
- Through the use of Internet Protocol Security

(IPsec), we can provide server and domain isolation.
- Through the application of storage-based segmentation and filtering methods, we can make use of encryption and LUN (Logical Unit Number) masking.
- When required, we can apply DSD-evaluated cross-domain solutions.

Why Network Segmentation is Important

The following explains the importance of network segmentation:

Boost Security: To guard against malevolent cyberattacks that can jeopardize the usability of your network. to identify and address an unidentified network incursion

Isolate network issues: In the event of an intrusion, offer a rapid method of separating a compromised device from the remainder of your network.

Decrease Congestion: The number of hosts per network can be decreased by dividing the LAN.

Expanded Network: By adding more routers, the network can be expanded, enabling more hosts to join the LAN.

WLAN

In the 1990s, wireless technology was first launched. Devices are connected to a LAN via it. In technical terms, it's known as the 802.11 protocol.

WLAN refers to wireless network connections via radio or infrared signals over short distances. WLAN is used as a brand name for Wi-Fi.

Any device connecting to a wireless local area network (WLAN) is referred to as a station and falls into one of two types.

- **Access Point (AP):** It is a device that can send

and receive radio frequency signals from other devices. These gadgets are typically routers.
- **Client:** It could include a range of gadgets, including desktop computers, IP phones, laptops, and workstations. BSS (Basic Service Sets) are all workstations that can establish connections with one another.

Types of WLAN

- Infrastructure
- Peer-to-peer
- Bridge
- Wireless distributed system

Important Components of WLAN

These components are crucial for WLAN to function as a wireless communication medium.

- Radio Frequency Transmission
- WLAN Standards
- ITU-R Local FCC Wireless
- 802.11 Standards and Wi-Fi protocols
- Wi-Fi Alliance

Installing, configuring, running, and switching networks.

Choosing and arranging the gear and equipment that will make up the network's framework and connective tissue is known as network installation.

Network-Based Installation: To create a unified, properly configured computer network, hardware and software must be planned, designed, and implemented.

Network Wiring Installation: To establish a dependable network and prevent maintenance issues, this type of highly specialized wire must be placed and arranged in a very particular manner.

Cabling Practices to Avoid

- Avoid running wires through holes and pipes since this may limit the number of cables that can be added in the future.
- Avoid over-twisting the cord.
- Copper cables have the potential to collapse fiber cables; thus, avoid placing them above or in the same runs as them.
- Avoid positioning cables in a way that makes it difficult for other equipment to enter or exit the racks.
- For effective cable management, never let cables lie around on the floor. Instead, utilize the overhead, vertical, and horizontal organizers.

How much does network wiring installation cost?

The scale of your project, the location, the quantity of gear needed, and the number of man hours needed to set up your new network will all affect the anticipated cost of installing network wiring.

- Wiring a large office building, which can have specific equipment that needs to be integrated into the network with separate data ports, costs between $2000 and $6000.
- Installing a hardwired computer network in a small office building can cost between $500 and $1000.

The capabilities and price points of the various types of wiring used to install a network vary:

- **Cat 5e Cable:** cost-cutting, slowest, and less reliable.
- **Cat 6e Cable:** suitable for small-scale projects; affordable; fast speed up to 10 GB for 90 meters long.
- **Cat 7 Cable:** most expensive, optimal performance, and top speed.
- **Fiber Optic Cable:** fastest of all the above, most reliable, and most expensive.

The type of network cable determines its price. Installing 2,000 feet of Cat 6 cable costs about $700, but Cat 7 cable costs about $1,200. Fiber optic cables typically cost $2 to $4 per linear foot, or $4,000 to $8,000 for 2,000 feet.

Network Installation and Configuration

Determine how much cabling your project will require first. Measure the distance between each node and the site you have chosen for your router and central server.

Step 1: Position Wall Plates

These wall plates need to be placed carefully since they are the conduits that connect your devices to the cabling that goes to your router. The ideal locations for wall plates are those that are easy to get to and stay away from other electrical fixtures like light switches and outlets.

Step 2: Make Wall Plate Holes

It’s crucial to stop the building’s power and turn off the appropriate switches in the breaker box before making any holes. It’s always better to measure twice and cut once when making holes.

Step 3: Connect the cable

Now is the time to run the cable between the terminal wall plates and the router while the power is still off. Occasionally, this necessitates entering the walls and ceiling of the building, particularly if it is an older structure that was not designed with cabling in mind.

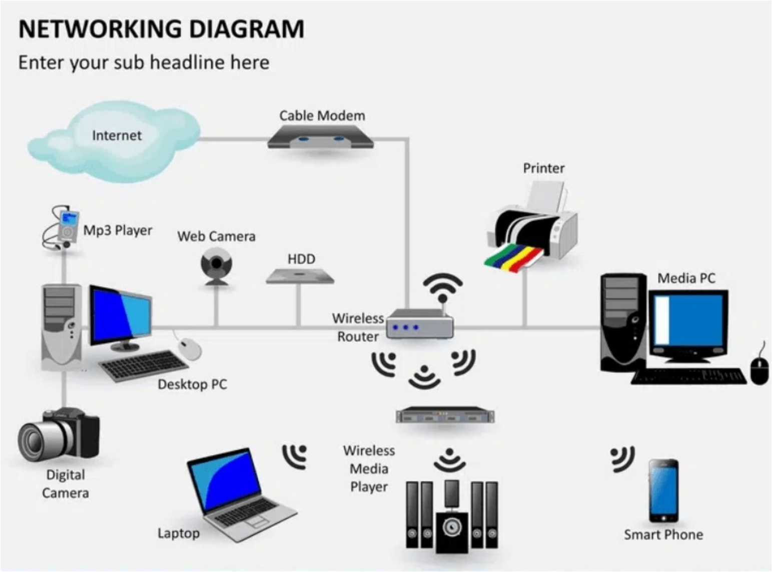
Step 4: Test Connection

Before connecting devices, make sure the network connection is working properly after the cable has been run through and linked on both ends. A network testing tool is used to achieve this, and it indicates whether or not the connection is active by flashing a sequence of lights.

Step 5: Network Configuration

You can start adding and configuring servers, routers, PCs, and other linked devices for security measures as soon as the network is up and running.

It is crucial that you or a professional, record the network installation process. Passwords, device names, network names, equipment lists, topology, and other pertinent data should all be included.



CCNA Tutorial

Network Configuration and Maintenance

If your company depends on a wired network for operation, maintenance is necessary to reduce downtime, ward against threats, and optimize the network's efficiency. These are some recommended procedures for maintaining networks:

- Thorough examinations of hardware and access points on a regular basis.
- Frequent upgrades to connected devices' software.
- Meticulous recording of every maintenance or troubleshooting event.

Network Cabling Best Practices

- Each cable should have a label at both the origin and the termination.
- When installing cables, make sure to test each one, identify any broken ones, and remove them.
- When bending cannot be avoided, use bend-loss-resistant cables.
- To prevent downtime, select network cabling that has enough vertical and horizontal runs.
- In confined areas, use thin, high-density cables to make more room available overall.
- To ensure fit, measure every patch cable carefully.
- Give each cable end a little leeway to accommodate device movement.
- To stop wires from bending and fraying, use cable spools inside equipment casings.
- Every two feet, gather cables together using Velcro ties—soft, flexible tie substitutes for zip ties.
- Map out the distribution of each cabling component and document it. Update your software to ensure constant connectivity.
- To manage cables properly, use cable guides.

Advanced Troubleshooting Techniques

Finding and fixing issues with connectivity, performance, security, and other network features is known as network troubleshooting.

What is the purpose of troubleshooting networks?

Today's networks carry out vital corporate functions. Networks are susceptible to expensive downtime in the absence of thorough troubleshooting and prompt issue resolution.

Reduced productivity, the financial effects of interrupted or failing services, malware, and data breaches are all included in the cost of downtime.

These repercussions may incur high expenses and harm brands over time.

How are troubleshooting procedures handled by organizations?

A huge organization dedicates a whole team to network issues. The engineers on the team handle issues at three different levels:

- Tier 1 is for routine problems like password resets.
- Tier 2 is for problems that Tier 1 is unable to handle
- Tier 3 is for issues that are crucial to the team's operations.

Tier 1 troubleshooting is often contracted out. To effectively channel requests and guarantee that upper-level engineers are assigned the right tasks, an escalation system is employed.

Automation, machine learning (ML), and artificial intelligence (AI) have all been utilized recently to close the skills gap. These solutions enable Tier 1 engineers to address complicated network issues more quickly by providing guided remediation tools.

Although many businesses already have their own dedicated network troubleshooting tools, adding these tools could necessitate IT staff managing and providing training. Network troubleshooting is more frequently integrated into network management systems (NMS).

Why NMS?

Network troubleshooting teams in large enterprises don't only wait for users to report problems.

- An NMS keeps a constant eye on networks. It provides status updates on network key performance indicators (KPIs) such as connection speed, bandwidth, latency, users, and access, along with alerts as necessary.

- The NMS polls its numerous nodes and components to update the network’s status at a time selected by the IT department.
- However, more recent network components use telemetry to automatically send their KPIs.
- Monitoring and gathering information on network events is a crucial component of network troubleshooting.
- This procedure makes use of an IT service management (ITSM) ticketing system.
- The information compiled from the tickets can help pinpoint issues and direct network upgrades and optimization.

Popular Network Troubleshooting Processes

After basic issues like hardware connections and user connectivity have been checked out and alarms or requests have been received, network troubleshooting usually entails one or more of the following procedures.

- **IP-configuration Checks:** Many network problems stem from issues with IP addresses. If a prior IP address is incorrect, a new one can frequently be assigned to fix the problem.
- **Ping and Tracert Testing:** The network problem can be upstream of a modem if the IP address is accurate. IT teams can use the tracert command or the ping utility to test connections with remote servers and provide information about the signal flow to further diagnose the issue.
- **DNS Checks:** If a DNS check is performed on a server that networks are attempting to connect to, it will reveal whether there is an issue. When an IT team does a DNS check and gets messages like “Request timed out” or “No response from server,” the destination DNS server may be the source of the issue.
- **Service Provider Checks:** Even with well-known cloud providers and cloud-based applications, outages still happen. Status

websites from providers list outages that could be impacting network performance.
- **Virus and Malware Checks:** Malware, including viruses, can impair network performance and are frequently difficult to identify. To check if any new attacks have been detected, IT teams should make use of security tools.
- **Database Logs:** Overloaded or full databases might cause network performance to lag. If this is the case, a new analysis of the database logs will demonstrate it.
- **Command-line Tools:** The two most used command-line utilities are nslookup and ipconfig. A plethora of other tools, including iptables, netstat, tcpdump, route, arp, and dig, can also be used to find network problems.
- **Test Environments:** IT teams may need to build test environments in order to replicate issues and validate fixes for particularly difficult cases or those involving private or restricted data.

Understanding of Automation and Security

The process of employing software to automate security, network provisioning and administration to continuously optimize network functioning and efficiency is known as network automation. Network virtualization and network automation are frequently combined.

Why network automation?

By automating network and security provisioning and administration over the whole application lifecycle and across data center and cloud environments, network automation helps you accelerate application deployment.

Streamline Your IT: Virtualize and automate network and security operations to further your digital transformation.

Accelerate the Creation of New Apps: Use DevOps techniques and brand-new cloud-native applications with networking and security controls that easily integrate into development workflows without requiring retooling.

See Clearly Across Environments: Trade in your historically constrained perspective of network traffic and security dependencies for worldwide visibility and simple network and security policy troubleshooting.

Examples of network automation

Software-defined networking (SDN) and network functions virtualization (NFV) technology are used in conjunction with network automation and virtualization to create and modify the network in accordance with business or service goals.

Network Security

The word "network security" is broad and encompasses a wide range of tools, equipment, and procedures.

It's a collection of guidelines and settings intended to safeguard computer networks and data accessibility, integrity, and confidentiality through the use of hardware and software technologies.

Three main controls are usually included in network security, as follows:

Physical Network Security: The purpose of physical security controls is to keep unauthorized individuals from physically accessing network equipment, including routers, cabling cabinets, and other items.

Technical Network Security: There are two aspects to protection: systems and data must be shielded against unauthorized users as well as hostile employee activity.

Administrative Network Security: Administrative security controls are made up of security guidelines and procedures that regulate user behavior, such as user authentication, access levels, and the way IT personnel make infrastructure modifications.

Types of Network Security

The following are a few methods you can use to safeguard your network:

- Network access control
- Antivirus and antimalware software
- Firewall protection
- Virtual private networks.

Any firm that handles networked data and systems ought to place a high premium on network security.

Conclusion

We hope this CCNA tutorial covers everything you are looking for in the fundamentals of networking. Get started with our **CCNA training in Chennai** for a promising career.

No.10, PT Rajan Salai, K.K. Nagar, Chennai – 600 078.
Landmark: Karnataka Bank Building
Phone: +91 86818 84318
Email: enquiry@softlogicsys.in
Map: Google Maps Link

OMR

No. E1-A10, RTS Food Street
92, Rajiv Gandhi Salai (OMR),
Navalur, Chennai - 600 130.
Landmark: Adj. to AGS Cinemas
Phone: +91 89256 88858
Email: info@softlogicsys.in
Map: Google Maps Link

Courses

- Python
- Software Testing
- Full Stack Developer
- Java
- Power BI
- Clinical SAS
- Data Science
- Embedded
- Cloud Computing
- Hardware and Networking
- VBA Macros
- Mobile App Development
- DevOps

- SLA's Recently Placed Students
- Reviews
- Sitemap

Important Links

- Disclaimer
- Privacy Policy
- Terms and Conditions

Social Media Links

Review Sources

- Google
- Trustpilot
- Glassdoor
- Mouthshut
- Sulekha
- Justdial
- Ambitionbox
- Indeed
- Software Suggest
- Sitejabber