Click to verify

Comptia network study guide

The Network+ Certification Study Guide will teach you the core skills necessary to establish, maintain, troubleshoot and secure networks regardless of technology or platform, empowering you to pursue a high growth career in networking and cybersecurity. After reading this text, you will be able to:Networking FundamentalsExplain basic networking concepts including network services, physical connections, topologies and architecture, and cloud connectivity. Network ImplementationsExplain routing technologies and networking devices; deploy ethernet solutions and configure wireless technologies. Network OperationsMonitor and optimize networks to ensure business continuity. Network SecurityExplain security concepts and network attacks in order to harden networks against threats. Network TroubleshootingTroubleshoot common cable, connectivity, and software issues related to networking. PrerequisitesTo get the most out of the CompTIA Network+ Study Guide and be able to prepare for your exam you ideally will have earned the CompTIA A+ certification and have about 9-12 months of experience of networking support or IT administration. It is not necessary that you pass the A+ exams before completing Network+ certification, but it is recommended.Regardless of whether you have passed A+, it is recommended that you have the following skills and knowledge before starting this course:Configure and support PC, laptop, mobile (smartphone / tablet), and print devices.Know basic network terminology and functions (such as Ethernet, TCP/IP, switches, routers).Configure and manage users, groups, and shared resources in a simple SOHO network.Understand the use of basic access control measures, such as authentication, security policy, encryption, and firewalls.Understand TCP/IP addressing, core protocols and troubleshooting tools. Article by Jane Newsom. Last Updated: Saturday, Sep 23, 2023.The CompTIA Network+ is a top tier IT certification that tells current or prospective employers that you've got what it takes. The certification comes from the same group that brings you the A+ and Security+ certs. If you're studying for these as well, checkout our handy A+ Study Guide and Security+ Study Guide reviews. It signifies an excellent grasp of Network design and implementation, troubleshooting, configuration and maintenance fundamentals.We'll cover the Network+ exam (N10-007) in detail, and give you our picks for the best CompTIA Network+ study guides, review guides, and practice tests to ensure your test prep success! The details are below, but if you just can't wait, here's the short list:Network+ Exam DetailsThe ComptTIA Network+ Exam (N10-007) covers current networking technologies across a broad range of topics.The exam is currently priced at $329, and is recommended for people with 9+ months of networking experience.The CompTIA Network+ covers networking topics, including security, infrastructure (cabling, devices, and storage), Operations and troubleshooting, and common tools.The exam is 90 minutes in length, and includes multiple choice (single and multiple response), drag and drop, and performance-based questions.You'll also be required to show proficiency in troubleshooting concepts, and best practices in change management, documentation, and scripting.ScoringThe CompTIA is administered by Pearson VUE, and your results will be calculated on completion of each exam automatically. It's scored on a scale of 100-900, and a passing score is 720.Best CompTIA Network+ Study GuidesThe Official CompTIA Network+ Study GuideEditor's ChoicePros: Complete and comprehensive review of all exam topics, direct from CompTIA.Cons: None of note.Our Rating: 5.0 / 5The Official CompTIA Network+ Certification Study Guide is our overall top pick for people studying for the Network+ Exam. As the name suggests, this is the official guide from the certification org, which means the material is the most reflective of what they expect you to know in order to pass the exams. All topics, including OSI Model, TCP/IP, security, access controls and more!The full list of features include:A complete look at all topics covered in the CompTIA Network+ Exam.Representative practice questions and tests so you know what to expect on test day.A strong, logical layout of material that's easy to digest.With incredibly strong content and essentially nothing in the negative column, this book is an easy recommendation for Network+ test prep. If this is your first time taking the exam (as opposed to a recertification), we strongly advise picking up this book. It's great as a stand-alone resource, or to compliment other materials. Either way, we're sure you'll love the results.CompTIA Network+ Deluxe Study GuidePros: Fantastic online resources, including practice tests and electronic flashcards.Cons: Organization isn't as strong as it could be.Our Rating: 4.5 / 5The CompTIA Network+ Deluxe Study Guide is our runner up pick, thanks in large part to excellent online supplemental material. The book itself is a comprehensive overview of critical test topics, and contains representative practice questions.The full list of features include:Detailed test-taking strategies and rationale for all practice questions.Offers invaluable insights and tips drawn from real-world experience.6 custom practice exams300 electronic flashcardsSearchable key term glossaryAccess to the Sybex online test bank, including hundreds of sample questions, a pre-assessment test, bonus practice exams, and over 300 electronic flashcardsWhile it didn't take the top spot, You'd still do well to consider this guide. It's a great compliment to the offical study guide that we mentioned as our top pick, and it's more abbreviated format makes it a perfect way to cram before your test!CompTIA Network+ All-in-One Exam GuidePros: A great condensed overview that's great for last minute prep.Cons: Not as comprehensive as other resources on this list.Our Rating: 4.5 / 5If you're short on time and need an accelerated review, or just going for recertification and want to brush up on a few topics, CompTIA Network+ All-in-One Exam Guide is a great pick for your specific needs. There's a special focus paid to the most critical topics, with all of the fluff and extras cut out.Features include:Contains complete coverage of every objective for the CompTIA Network+ Certification exam.Electronic content includes the Total Tester exam simulator with over 100 practice questions.Over an hour of training videos, and a collection of Mike Meyers' favorite shareware and freeware networking utilitiesIt might not be enough to pass the exam if you aren't already a seasoned Networking professional. If you are, or this is supplementing some of the more in-depth guides, then this is a good choice. By restricting its focus to just the relevant topics, it can't be beat!CompTIA Network+ Exam CramPros: Another abbreviated review for both exams that still manages to touch all topics.Cons: Not as comprehensive as the more expensive study systems above.Our Rating: 4.5 / 5The CompTIA Network+ Exam Cram is another good option for abbreviated review. The name says it all, if you're looking for a little last minute cramming, this is what you need! Through a narrowly tailored focus, this book helps you drill down on topics where you need the most help in the days leading up to the test.Features include:The companion website contains the powerful Pearson Test Prep practice test software, complete with hundreds of exam-realistic questions.Coverage and practice questions for every exam topic, including substantial new coverage of security, cloud networking, IPv6, and wireless technologies.Well organized test-preparation routine through the use of proven series elements and techniques.As with the book above, we don't recommend this as your only guide unless it's a recertification or you're already a pro. That said, the narrow focus can be a great help in the final days, since it can be easier to review the more condensed material.Wrapping UpFor IT Professionals, the Network+ Certifications is a great way to signal to current and prospective employers that you can design, deploy, operate and maintain networks. It's one of the few vendor agnostic certifications that has the same notoriety as counterparts like the CCNA.Study manuals, flashcards, and practice tests are a huge help to many people, and if you've read this far you're probably one of them.We've rounded up the top Network+ study guides and presented them above.Our top pick for most people is The Official CompTIA Network+ Certification Study Guide. It's the most comprehensive and accurate guide on our list, produced by CompTIA, and is the single best resource available.For those shorter on time, or just needing a quick review, the Exam Cram book is a safe bet for touching on all the most critical aspects.Whatever your circumstance, supplemental study and review materials are a key part of ensuring success. We've listed some of the best books available. Good luck, and study hard! Welcome to your free CompTIA Network+ study guide. Full explanations and examples Written by network experts Exam tips and real-world advice included Learn wireless, network security, switching, troubleshooting, routing and more We cover most of the CompTIA Network+ N10-008 syllabus here but it's from a previous version of the exam so you will need to supplement your learning with some further research or take our video and lab based Network+ course. Please read this blog post if you want to know what's covered in the N10-008 exam syllabus. Feel free to check out our hands-on Network+ lab training book on Amazon below: Video training courses for the Network+ exam can be found in the menu at the top of the page. Section I – NETWORKING CONCEPTS Chapter 1 – OSI Model vs TCP Model Chapter 2 – Matching Network Components with OSI Layers Chapter 3 – IP Addressing Chapter 4 – Routing Protocols and Switching Chapter 5 – Port Numbers and Network Protocols Chapter 6 – Network Troubleshooting Chapter 7 – Network Virtualization Section II: NETWORK INSTALLATION AND CONFIGURATION Chapter 8 – Configure Routers and Switches Chapter 9 – Wireless Network Configuration Chapter 10 – What is DHCP? Chapter 11 – Wireless Problems and Troubleshooting Chapter 12 – Troubleshoot Routers and Switches Chapter 13 – SOHO Networks Section III: NETWORK MEDIA AND TOPOLOGIES Chapter 14 – Network Cabling and Standards Chapter 15 – Network Cable Connectors Chapter 16 – Wide Area Networks Chapter 17 – Network Topology Types Chapter 18 – Physical Connectivity Troubleshooting Chapter 19 – Ethernet Standards Chapter 20 – Wiring Distribution Section IV: NETWORK MANAGEMENT Chapter 21 – Network Appliances Chapter 22 – Hardware Troubleshooting Tools Chapter 23 – Software Troubleshooting Tools Chapter 24 – SNMP – Syslog – Network Traffic Analysis Chapter 25 – Network Documentation Chapter 26 – QoS and Network Performance Section V: NETWORK SECURITY Chapter 27 – Wireless Security Chapter 28 – Securing Network Access Chapter 29 – User Authentication Chapter 30 – Common Threats and Vulnerabilities Chapter 31 – Types of Firewalls Chapter 32 – IDS vs IPS Section VI: NETWORK+ PRACTICE TESTS Network+ Practice Test 1 Network+ Practice Test 2 Compare the layers of the OSI vs TCP/IP models. The first chapter in the Networking Concepts section proposes an analysis of the OSI and TCP/IP models, taking into account the particularities of each of the seven OSI layers and the four TCP/IP layers. The information presented in this chapter will help students understand the logical process that happens when network devices communicate with each other. The OSI and TCP/IP models were defined in order to understand and structure the processes that make a network function. While the OSI (Open System Interconnection) reference model can help in understanding how network communications occur, it represents more of a theoretical approach, unlike the TCP/IP (Transmission Control Protocol/Internet Protocol) protocol suite used in production. TCP/IP is considered a set of protocols (or a protocol stack) that operate together to accomplish various tasks that allow inter-communication among network devices. Learn more in the CompTIA Network+ course. Back to book index. The OSI Reference Model The OSI reference model was defined in ISO/IEC 7498-1. It is a seven-layer model used in networking, a layered mechanism that describes how information from an application on a network device (e.g., computer, router, etc.) moves from the source to the destination using the physical medium, and then interacts with the software application on that specific network device, as illustrated in Figure 1.1 below: Figure 1.1 – OSI Reference Model OSI was developed by the International Organization for Standardization (ISO) in 1984. The OSI mechanism involves two concepts: The OSI reference model, which has seven layers The OSI protocols that map to each of the seven layers In other words, the OSI model defines the network functions required for sending data and divides them into seven categories. The seven layers of the OSI reference model, starting from the top (i.e., Layer 7), are shown in Table 1.1 below: Table 1.1 – The OSI Reference Model OSI Layers Layer 7 Application Layer 6 Presentation Layer 5 Session Layer 4 Transport Layer 3 Network Layer 2 Data Link Layer 1 Physical The upper layers involve application issues, such as interfacing with the user or formatting data. The lower layers relate to transport issues, such as data routing and the physical characteristics of the network. When a network device (source) communicates with another network device (destination), the information flows as presented in Figure 1.1 above, starting from the source device's Application Layer, going down to its Physical Layer, arriving at the destination device's Physical Layer, and going up to its Application Layer. The response from the destination device to the source device follows the reverse order: Layer 7 to Layer 1 and then Layer 1 to Layer 7. It is really essential to understand the OSI reference model from a design standpoint because of its modular architecture. The OSI model divides the specific tasks that are involved in moving information from one networking device to another into seven smaller and more manageable groups of tasks/actions. The overall goal of the OSI model is to enhance interoperability and functionality between different applications and vendors, as well as to make it easier for network administration to focus on the design of particular layers of the model. For example, applications can be designed without having to worry about the lower OSI layers, so a certain level of trust is present if the packet has already been analyzed by the lower layers. The same rule applies in the other direction: the Application Layer trusts that the lower layers will successfully process and send the packet over the wire. The OSI reference model is a key concept in the networking industry and it plays an important role in the design phase of a network using a modular (layered) approach. Note: The OSI reference model represents everything that must happen in order to send data, but it does not specify how these things are done. Different protocols implement these functions differently at various layers and the OSI model provides a framework for these communication protocols to be used between devices. Protocols A protocol is a set of rules. Network devices need to agree on a set of rules in order to communicate and they must use the same protocol to understand each other. A wide variety of network protocols exist at different OSI layers. For example, at the lower OSI layers, LAN and WAN protocols are used. Going up the reference model, routed and routing protocols are found at Layer 3. Each layer and its associated protocols will be covered in detail in the following sections. Protocols can be organized in protocol suites or stacks. TCP/IP is the most commonly used network protocol suite, named after the two protocols in the stack. The TCP/IP protocol suite can be found in almost all modern networks, and it is a core feature not only of the Internet but also within organizations' networks. Other examples of protocol suites are AppleTalk and Novell NetWare. OSI Application Layer The Application Layer (Layer 7) is the layer closest to the end-user, who utilizes the network services available. For example, to transmit information such as data requests, pictures, and document files, the end-user interacts directly with an application in the Application Layer, which manages software applications that have communication-over-internetwork functionality. Depending on the information the user wants to send over the network, a specific protocol is used at the Application Layer. A few examples include the following: SMTP, POP3: used to send/receive an e-mail message FTP: used to transmit a file over the network Telnet: used to control a remote device OSI Presentation Layer The Presentation Layer is Layer 6 and it makes sure that the data is understandable to the end-system. In other words, the data must be converted and formatted in such a way that the system recognizes it and knows how to treat it. This includes the translation and conversion of details like formatting, compression schemes, encryption schemes, and character representation formats (e.g., ASCII to Unicode). Most often, the Presentation Layer will handle conversion schemes and video and audio compression (e.g., MPEG, AVI, JPEG, GIF, and TIF files). If the packets from the Application Layer are sent unformatted, the Presentation Layer translates them and then passes them to the Session Layer. Layer 6 specifies the format, data structure, coding, compression, and other ways to represent the data to ensure that information sent by a host at the Application Layer can be properly interpreted by the destination host. OSI Session Layer From a technical standpoint, communications systems are made up of different service requests and service responses between applications located on different networking devices. The Session Layer (Layer 5), establishes, manages, and terminates these communication sessions and connects the lower layers with the Presentation and Application Layers. It negotiates these connections, makes sure that the device is willing to talk to the other party, and tracks the conversation using port numbers. OSI Transport Layer The middle stack layer, the Transport Layer (Layer 4), accepts data from the Session Layer and breaks it up into transport segments. The Transport Layer is responsible for the information reaching the destination device in an error-free fashion and in the proper order (i.e., the correct sequence of packets), utilizing the following features to accomplish this task: Reliability Transmission error checking Error correction Data retransmission Flow control Sequencing Data multiplexing From a technical standpoint, all of these features are implemented by establishing a virtual circuit between the sender and receiver devices. The Transport Layer initiates, maintains, and terminates these virtual circuits at OSI Layer 4 and uses segments as the protocol data units (PDUs). Segments are defined sets of data that include control information and they are sent between the Transport Layers of the endpoints. The following two protocols in the Transport Layer are used on the Internet: Transmission Control Protocol (TCP): a reliable, connection-oriented protocol User Datagram Protocol (UDP): an unreliable, low overhead, connectionless protocol Connection-oriented protocols establish a logical connection and use sequence numbers to ensure that all the data is received at the destination. Connectionless protocols only send the data, relying on the upper-layer protocols to handle error detection and correct possible problems. Note: The process of segmenting the data is transparent to the upper layers, as the Transport Layer at the other end will re-assemble everything before passing the data over to the Session Layer. OSI Network Layer Layer 3, also known as the Network Layer, is responsible for identifying the internetwork path (routing) from the sender device to the receiver device. Considering this aspect, Layer 3 is responsible for the logical addressing schemes (e.g., IP, IPX, and AppleTalk) that assign logical addresses to the network hosts on both sides of the communication path. The Network Layer sends datagrams (or packets), which are a defined set of data that includes addressing and control information. Datagrams are routed between source and destination devices. If a datagram needs to be sent across a network that can handle only a certain amount of data at a time, it can be fragmented into multiple packets and reassembled by the receiving device. In other words, a datagram is considered a unit of data and a packet is what physically goes on the network. If no fragmentation occurs, a datagram is a single packet. In addition to logical addressing schemes, the Network Layer is also responsible for route selection and packet forwarding, and it deals with two types of protocols: Routed protocols: IP, IPX/SPX, AppleTalk, and DECnet Routing protocols: RIP, EIGRP, OSPF, IS-IS, and BGP Routed protocols are responsible for the actual rules and processes involved in the encapsulation of the data packets that are ultimately routed over the internetwork. Routing protocols find available routes that exist on the network, build routing tables, and make routing decisions. Network devices that operate at Layer 3 are called routers. OSI Data Link Layer Layer 2 (Data Link Layer) defines the format of data that is transmitted across the physical network and encapsulates it based on the media type. A frame represents the organization of data in a specific fashion so that both parties can understand it, and the Data Link Layer chooses the proper frame type based on the link in use. The Data Link Layer has two sublayers: the Logical Link Control (LLC) sublayer and the Media Access Control (MAC) sublayer. The LLC sublayer deals with the Network Layer, while the MAC sublayer has access to physical media in the Physical Layer (Layer 1). These sublayers are shown in Figure 1.2 below: Figure 1.2 – Data Link Sublayers The LLC sublayer (IEEE 802.2) allows multiple Network Layer 3 protocols to communicate over the same physical link by allowing those protocols to be specified in the LLC fields. The MAC sublayer (IEEE 802.3) specifies the physical MAC address that identifies a device on a network. Each frame sent over the wire contains a MAC Address field and only those devices with that specific MAC address will process the frame. A Source MAC Address field is also included in the frame. The Data Link Layer offers reliable transmission of data across a physical network link and allows different Data Link Layer specifications that provide different network and protocol characteristics. This includes physical addressing, different network topologies, error notifications, frame (Layer 2 data units) sequences, and frame flow control. Layer 2 manages physical addressing, while Layer 3 handles logical addressing. Physical addressing is generally in the form of MAC addresses (burned into a computer network interface card (NIC) or in the interfaces of network devices). MAC addresses are 48 bits long and the standard format contains six groups of two hexadecimal digits separated by hyphens (-) or colons (:), for example, aa:bb:12:34:56:67 or aa-bb-12-34-56-67. Every device on the network has a unique physical address that has to be included in the message so it can be delivered to the proper device. If the physical address of the destination is not known, the packet will be forwarded to all the devices on that segment. Network devices that operate at Layer 2 are called switches. Note: MAC addresses are also called burned-in addresses (BIAs) or hardware addresses. OSI Physical Layer The Physical Layer is placed at the bottom of the OSI protocol stack and it represents the actual physical medium on which the information is traveling between network devices. Layer 1 interconnects with the Data Link Layer through the Layer 2 MAC sublayer and sends the physical signals that encode 0 and 1 bits, or "binary digits" (i.e., electrical signals over copper links, fiber-optic light beams, and radio frequencies for wireless transmissions). The protocols that operate at the Physical Layer include the following: Local Area Network (LAN) protocols: Ethernet,* IEEE 802.3, 100BaseT, Token Ring/IEEE 802.5, and FDDI Wide Area Network (WAN) protocols: EIA/TIA-232, EIA/TIA-449, V.35, and EIA-530 Layer 1 defines physical media procedures, electrical or mechanical aspects, encoding, and modulation (voltage) on the line, and the electrical signal generated either will be a 0 or a 1 bit or will be placed into a transition state. The Physical Layer also activates, maintains, and deactivates the actual physical links between multiple systems in LAN and WAN networks. *Ethernet actually operates at both Layer 1 and Layer 2 of the OSI reference model. Note: Every process and function within Layers 2 to 7 of the OSI reference model (or Layers 2 to 4 of the TCP/IP protocol suite) happens logically inside the network device, whereas Physical Layer (TCP/IP Network Access Layer) functionality transmits bits as electrical signals on the wire, light beams on fiber-optic links, or radio frequencies in Wi-Fi networks. Encapsulation In both LANs and WANs, packet transmission can be analyzed using the seven-layer OSI reference model. When data is transmitted by the source toward a specific destination, it passes through the Application, Presentation, and Session Layers and the PDU arrives at Layer 4 (Transport Layer). The process of sending data down the protocol stack (from the Application Layer to the Physical Layer) is called encapsulation. The upper layer sends data down to the next level, which adds its own specific information (using a header and a trailer) before sending it down to the next layer where the process is repeated, making the message bigger at each layer. The opposite process is called decapsulation, in which the destination device receives the message and moves it up the protocol stack to the Application Layer. As the message travels through the layers, each layer removes the lower layer's additional information (i.e., header and trailer), making the message smaller as it goes up the protocol stack. As illustrated in Figure 1.3 below, the Transport Layer (Layer 4) places a 20-byte header in front of the data. Regardless of the protocol used (i.e., TCP or UDP), the Layer 4 header and the data form a segment that is passed down to Layer 3 (Network Layer). The Network Layer places its header in front of the segment received and this group becomes a packet (or a datagram). The Layer 3 header contains very important fields that include the logical address (IP address) of both the source and destination device. The newly formed packet is passed down to Layer 2 (Data Link Layer), which creates a new data unit (i.e., a frame) by adding the Layer 2 frame header and trailer. The frame is then passed down to the Physical Layer (Layer 1), which converts the information into 0 and 1 bits that are sent over physical media using, for example, electrical signals (for a copper link). Finally, the data is sent over the wire using a wide variety of methods, such as Ethernet, Token Ring, or other technologies. The headers and trailers used in the encapsulation process contain specific control information that allows the data to go through the network properly. Thus, the data at each layer is encapsulated by information appropriate for that specific layer, including addressing and error checking. Figure 1.3 – Packet Encapsulation A protocol data unit (PDU) is a group of data used to exchange information at a particular OSI layer. The Layer 1 to Layer 4 PDU types, signifying the group of data and the specific headers and trailers, are summarized in Table 1.2 below: Table 1.2 – PDU Types Layer PDU Types Layer 1 Bit Layer 2 Frame Layer 3 Packet (Datagram) Layer 4 Segment To summarize, referring to Figure 1.3, with encapsulation the amount of information increases as the data travels down through the lower layers to the Physical Layer (as shown on the left). With decapsulation the destination device receives the data and this additional information is analyzed and then removed as the data is passed up through the higher layers to the Application Layer (as shown on the right). In addition to the Layer 3 logical addressing fields in the header, an addressing structure is also applied in the Layer 2 header (i.e., the MAC address). Every network device has a physical BIA located in a special field in the Data Link Layer header. This address changes as the packet passes from one device to another (e.g., from the source PC to the switch to the router to another switch and, finally, to the destination PC), but the original IP source and destination addresses do not change when transiting the network because the packet is stripped of its Layer 3 header once it goes beyond a router. When a packet stays within the same LAN, it passes through switches only and is decapsulated until it reaches the Layer 2 header, which contains the MAC address. This header changes as the packet is re-encapsulated, as do the MAC address fields. Finally, different protocols are available at each layer. For example, IP packets are different from IPX packets. Proper network operation implies that both the source and the destination endpoints are communicating using the same protocol. TCP/IP Protocol Suite Although the OSI model does a great job of describing in detail how the network operates, it is actually considered a reference model. To ensure proper communication between network devices, the TCP/IP protocol suite is used instead. Note: The OSI reference model was created by the International Organization for Standardization (ISO), while the TCP/IP protocol suite was created and first implemented by the Internet Engineering Task Force (IETF). The TCP/IP protocol suite is a modern adaptation of the OSI reference model and it contains five layers: Application Layer Transport Layer Internet Layer Data Link Layer Physical Layer In some documentation, the Data Link Layer and the Physical Layer are combined into a single layer called the Network Access Layer or the Network Interface Layer. Figure 1.4 below shows the TCP/IP protocol suite next to the OSI reference model: Figure 1.4 – TCP/IP Protocol Suite TCP/IP Application Layer The Application Layer in the TCP/IP protocol suite covers the functionality of the Session, Presentation, and Application Layers in the OSI reference model. Various protocols can be used at this layer, among which include the following: SMTP, POP3: used to provide e-mail services HTTP: World Wide Web browser content delivery protocol FTP: used in file transfers DNS: used in domain name translation SNMP: network management protocol DHCP: used to automatically assign IP addresses to network devices Telnet: used to manage and control network devices TCP/IP Transport Layer Both the TCP/IP Transport Layer and the Internet Layer display considerable differences when compared with the corresponding OSI layers. The Transport Layer is based on two protocols: Transmission Control Protocol (TCP): This protocol provides a connection-oriented transmission. This means that the path the data travels on through the network is reliable, as the endpoints establish a synchronized connection before sending the data. Every data packet is acknowledged by the receiving host. File Transfer Protocol (FTP) is an example of a protocol that uses TCP. User Datagram Protocol (UDP): This protocol provides an unreliable, connectionless transmission between hosts. Unlike TCP, UDP does not check the segments that arrive at the destination to make sure that they are valid and in the proper order. This means that integrity verifications and the error correction process will occur at the Application Layer. On the other hand, UDP has a smaller overhead compared with TCP because the UDP header is much smaller. Trivial File Transfer Protocol (TFTP) is an example of a protocol that uses UDP. The TCP and UDP protocol data units are segments, and each segment contains a number of fields that carry different information about the data, as shown in Figure 1.5 below: Figure 1.5 – UDP and TCP Segment Fields The UDP fields are described in Table 1.3 below: Table 1.3 – UDP Fields Field Size Description Source Port Number 16 bits Identifies the application used by the sender Destination Port Number 16 bits Identifies the application used by the receiver Length 16 bits The size of the header and the data Checksum 16 bits The checksum of the header and the data, used to verify integrity of the segment Data Variable Application data The TCP fields are described in Table 1.4 below: Table 1.4 – TCP Fields Field Size Description Source Port Number 16 bits Identifies the application used by the sender Destination Port Number 16 bits Identifies the application used by the receiver Sequence Number 32 bits Verifies the correct order of segments received Acknowledgement Number 32 bits Verifies the correct order of segments received Header Length 4 bits The size of the header Reserved 6 bits Unused field Code Bits 6 bits Indicates the segment type Window Size 16 bits The number of bytes received before sending an acknowledgement Checksum 16 bits The checksum of the header and the data, used to verify integrity of the segment Urgent 16 bits Marks the end of urgent data Option 0 to 32 bits Defines the maximum TCP segment size Data Variable Application data The TCP header is larger than the UDP header because extra fields are needed to ensure a reliable connection. Port numbers can have values up to 65535. Most of the common applications are assigned well-known port numbers, which are 0 to 1023. Port numbers 1024 through 49151 are registered port numbers, and the range of 49152 to 65535 defines dynamic port numbers (automatically assigned by network devices). Port numbers are used to distinguish applications running on the same device. Examples of well-known port numbers include the following: HTTP: TCP port 80 FTP: TCP port 20 (data) and port 21 (control) TFPT: UDP port 69 POP3: TCP port 110 SMTP: TCP port 25 DNS: TCP and UDP port 53 SNMP: UDP ports 161/162 Telnet: TCP port 23 When a TCP connection is established, it follows a process called a three-way handshake. This process uses a TCP segment with SYN and ACK bits, and this segment includes the Code Bits, Sequence Number, and Acknowledgement Number fields. The three-way handshake process is illustrated in Figure 1.6 below: Figure 1.6 – TCP Three-Way Handshake Process In Figure 1.6 above, Host A tries to establish a TCP connection with Host B. Host A sends a segment with a SYN bit set, letting the other device know that it wants to synchronize, and this segment includes the initial sequence number that Host A is using, which is 5. Host B accepts synchronization with Host A and sends back a segment with a SYN bit set and an ACK bit set to acknowledge that it has received the initial segment sent by Host A. The acknowledgement number sent by Host B represents the next segment it expects to receive, which is 6 (this is also called an expectational acknowledgment). The new segment also includes the initial sequence number that Host B is using, which is 14. Host A replies with an ACK segment that contains a sequence number of 6 (because that is what Host B is expecting) and an acknowledgement number of 15, informing Host B that it can send the next segment. This concludes the TCP session establishment phase. During the window size negotiation phase, the remote host learns the number of bytes a device will accept before it must send an ACK. The window sizes of the two endpoints may not match, so negotiation must take place. In Figure 1.6, Host A has a window size of 2 and Host B has a window size of 3. When Host A sends data, it can send 3 bytes before waiting for an ACK, while Host B can send only 2 bytes before receiving an ACK. Note: The Window Size field specifies the number of bytes (octets) a device will accept, not the number of segments. After all the data has been sent between the two hosts during the data transmission phase, the session closing phase begins. Host A sends a segment with a FIN bit set, letting Host B know that it wants to end the TCP session. This segment includes the sequence number Host B is using at that specific moment, which is 341. Host B acknowledges the request and sends an ACK bit set with an acknowledgement number of 342 to confirm that it received acknowledgement number 341. This segment also includes the current sequence number of Host B, which is 125. Host B sends a new segment with a FIN bit set, announcing that the application it is running also requests an end to the session. In the last step before the session is closed, Host A sends an ACK segment with the number 126 to confirm that it received number 125 from Host B. TCP/IP Internet Layer The Internet Layer in the TCP/IP protocol suite corresponds to OSI Layer 3 (Network Layer) and includes the following protocols: Internet Protocol (IP): This protocol is a connectionless protocol that offers best-effort delivery of packets in the network. It relies on Transport Layer protocols such as TCP to ensure a reliable connection. IP addresses are assigned to each network device or interface in the network. The IP protocol comes in two flavors: IPv4 and IPv6. These aspects will be covered in detail later in this book. Internet Control Message Protocol (ICMP): This protocol sends messages and error reports through the network. The most commonly used application that relies on ICMP is ping. The ping application sends an ICMP Echo Request message to the destination and expects an ICMP Echo Reply back to test that the destination can be reached and to get information about any delays between the two endpoints. TCP/IP Network Access Layer The Network Access Layer is comprised of the Data Link Layer and the Physical Layer and has the same functionality as the same two layers in the OSI reference model. A common protocol used at the Data Link Layer is the Address Resolution Protocol (ARP), which requests the MAC addresses of a host with a known IP address. Once the MAC address is known, it is used as a destination address in the frames sent in that specific direction. Traffic Analysis In this section we will analyze a specific example that involves a communication flow (i.e., an FTP Request) between two network devices, specifically an FTP client and an FTP server, as depicted in Figure 1.7 below: Figure 1.7 – Traffic Flow Example Note: This example presents an FTP Request packet but the specific Application Layer information is not relevant in analyzing the overall layer structure in a generic packet. Traffic flow in this example will be analyzed from the perspective of the TCP/IP layers, as inspected by traffic analyzer software (Wireshark in this case) that captures packets as they are transmitted over the wire between the two devices. Figure 1.8 – Traffic Analysis of the Overall Layer Structure Figure 1.8 above shows the overall TCP/IP layers as presented by the traffic analyzer, with the Network Access Layer divided into the Physical Layer and the Data Link Layer. Each line in the output above represents a specific TCP/IP layer, as follows: First line: Physical Layer Second line: Data Link Layer Third line: Network Access Layer Fourth line: Transport Layer Fifth line: Application Layer Next, each layer will be described in detail as it is presented by the traffic analyzer, starting with the Physical Layer. Traffic Analysis – Physical Layer Figure 1.9 – Traffic Analysis of the Physical Layer The Physical Layer fields in Figure 1.9 above contain information about the actual packet signaling and bits as they are passed over the wire. Of particular importance is the total number of bits included on the first line, which is 576 bits. The remaining output in Figure 1.9 is not relevant at the moment. Traffic Analysis – Data Link Layer Figure 1.10 – Traffic Analysis of the Data Link Layer The Data Link Layer presented in Figure 1.10 above shows the following important Layer 2 (Ethernet in this case) information: Destination device MAC address (Layer 2 address): 00:ff:58:fd:fa:0b (FTP server) Source device MAC address (Layer 2 address): 00:ff:57:fd:fa:0b (FTP client) EtherType: 0x0800, indicates which protocol is encapsulated in the payload of the Ethernet Frame (IPv4 in this case) Traffic Analysis – Network Access Layer Figure 1.11 – Traffic Analysis of the Network Access Layer As shown in Figure 1.11 above, Layer 3 contains relevant information about the Network Access Layer protocol used, which is IPv4 in this case. The information structure of Layer 3 correlates with the IPv4 packet structure that will be presented in subsequent sections. This includes IP addressing information and other Layer 3 overhead: Internet protocol version: 4 (identifying IPv4) Header length Differentiated Services field (QoS marking) Total packet length Identification, flags, and fragment offset TTL (Time To Live) information Transport Layer protocol: TCP in this case Header checksum Source IP address: 10.7.0.6 (FTP client) Destination IP address: 192.168.1.250 (FTP server) Traffic Analysis – Transport Layer Figure 1.12 – Traffic Analysis of the Transport Layer As shown in Figure 1.12 above, the Transport Layer contains information about the Layer 4 protocol in use: TCP in this case. Because TCP is a reliable protocol, it uses the overhead of sending sequence numbers and acknowledgements. The tracking information includes the following fields: Source Port Number (random high port number) Destination Port Number (FTP port 21) Sequence Number Acknowledgement Number Window Size Flags Checksum Note: Port numbers are assigned by the Session Layer when the transmission parameters are negotiated to ensure that the data goes to the proper application on the destination device. Traffic Analysis – Application Layer Figure 1.13 – Traffic Analysis of the Application Layer The Application Layer contains relevant information related to the specific application used (i.e., service provided for the user) and the specific packet type, which is an FTP Request in this case. Summary The OSI reference model and the TCP/IP protocol suite were defined in order to understand the structure and the processes that make a network function. While the OSI reference model is beneficial for describing how network communications occur, it represents more of a theoretical approach, unlike the TCP/IP protocol suite used in production. The TCP/IP approach to network communications is comprised of a set of protocols that operate together to accomplish various tasks that allow network devices to communicate with each other. The seven layers of the OSI reference model and the corresponding five layers of the TCP/IP protocol suite, starting from the top, are shown in Table 1.5 below: Table 1.5 – TCP/IP Layers Mapped to the OSI Layers OSI Layers TCP/IP Layers (7) Application Application (6) Presentation (5) Session (4) Transport Transport (3) Network Internet (2) Data Link Data Link (1) Physical Physical The OSI model is a key concept in the networking industry and it plays an important role in the design phase of a network using a modular (layered) approach. A protocol is a set of rules. Network devices need to agree on a set of rules in order to communicate and they must use the same protocol to understand each other. A wide variety of network protocols exist at different OSI layers. For example, at the lower OSI layers, LAN and WAN protocols are used. Going up the reference model, routed and routing protocols are found at Layer 3. The process of sending data down the protocol stack is called encapsulation. Data sent by the upper layer is received by each subsequent layer, which adds its own specific information. The opposite process is called decapsulation; after the destination device receives the message, it analyzes and removes information as it moves up through the protocol stack. A PDU is a group of data used to exchange information at a particular OSI layer. The Layer 1 to Layer 4 PDU types, signifying the group of data and the specific headers and trailers, are summarized in Table 1.6 below: Table 1.6 – PDU Types Layer PDU Types Layer 1 Bit Layer 2 Frame Layer 3 Packet (Datagram) Layer 4 Segment OSI model on Wikipedia.

- bifide
- nuhewibo
- tenis para o dia a dia feminino
- beyanu
- https://kubusiowadolina.pl/userfiles/file/50735671979.pdf
- vestido de madrinha de casamento longo
- http://altodelaciudad.com/userfiles/file/29401438688.pdf
- horário do ônibus taquaraçu de minas 4442
- pijatatowi