11110 Packet Tracer Implement Port Security

Packet Tracer 11.1.10: Implementing Port Security – A Comprehensive Guide

This guide provides a comprehensive walkthrough of implementing port security on a Cisco Packet Tracer network using the 11.1.10 scenario. It covers the theory behind port security, step-by-step instructions, best practices, and common pitfalls. Understanding port security is crucial for network security, preventing unauthorized access to switch ports and limiting potential threats like MAC flooding and denial-of-service attacks.

Understanding Port Security

Port security, a feature of Cisco switches, restricts access to a port based on the MAC addresses of devices connected to it. This prevents unauthorized devices from connecting and ensures only trusted devices gain access. It works by creating a MAC address table for each port. Once configured, the switch only allows traffic from authorized MAC addresses.

Scenario Overview (11.1.10)

The scenario typically involves configuring a switch to secure a specific port using MAC address static binding. This guide assumes a standard network topology likely featuring a switch and multiple PCs.

Step-by-Step Implementation

1. Identify the Network Topology: Carefully examine the Packet Tracer topology to understand the device connections and desired security restrictions.

2. Access the Switch Configuration: Open the CLI (Command-Line Interface) of the switch using Packet Tracer's interface.

3. Configure Port Security:
Enter Global Configuration Mode: Type `configure terminal`.
Navigate to the specific port: Use the `interface` command to enter the interface configuration mode, for example: `interface GigabitEthernet0/1`.
Enable Port Security: Use the `switchport port-security` command. This command enables port security on the interface.
Specify the Maximum Number of MAC Addresses: Using the `switchport port-security maximum` command, define the maximum number of allowed MAC addresses. (e.g.,

`switchport port-security maximum 2`)
Enable Port Security Violation: `switchport port-security violation restrict` or `shutdown` (better for production) to define the action if a violation occurs.
Add Static MAC Address Entries: Use the `switchport port-security mac-address` command to specify the permitted MAC addresses. (e.g., `switchport port-security mac-address 0000.0C07.AC12`) Repeat for each permitted address.
Confirm Configuration: Use the `show running-config` command to verify that the port security settings are correctly applied.

4. Verify Configuration: After entering all the commands, verify the configuration using `show running-config`.

5. Connect Devices: Connect the computers/devices with the permissible MAC addresses to the configured port to test the setup.

Best Practices

Detailed Documentation: Document the MAC addresses explicitly, their corresponding ports, and the security rules.
Regular Audits: Regularly update the MAC address table to reflect changes in the network environment.
Redundancy: Consider using a backup switch or VLANs to mitigate potential interruptions if a protected port malfunctions.
VLAN Segmentation: Secure ports with VLANs to further restrict network access.
Monitoring: Monitor ports for any security violations for proactive issue detection.

Common Pitfalls to Avoid

Incorrect MAC Addresses: Ensure that the MAC addresses are correctly entered. Errors here will prevent legitimate devices from connecting.
Missing Commands: Check for missing or incorrectly ordered commands. Example: forgetting to enable port security.
Wrong Mode: Confirm you're in the correct mode – Global Configuration, Interface Configuration.
Maximum Violations: Be aware of the consequences of exceeding the allowed MAC addresses.

Troubleshooting

If a device cannot connect, check:
Correct MAC Address: Verify the MAC address used matches the one entered on the switch.

Port Security Violations: If the switch is configured to shut down the port on violation, check if a violation occurred.
Wrong Configurations: Review and carefully examine all commands in the configuration for errors.

Example

Imagine a network with a switch port connected to a server and two workstations. You want to secure the port to only allow access from the server and two workstations. Use MAC addresses for each device and enter the commands accordingly.

Summary

Implementing port security in Packet Tracer 11.1.10 helps significantly enhance network security by restricting unauthorized access to switch ports. Following the steps and best practices ensures a secure network environment, preventing potential threats, and minimizing downtime.

FAQs

1. Q: What happens if a non-authorized MAC address tries to connect to the port?
A: If the switch is configured for "restrict," the attempt will be denied. If it's configured to shut the port down, the port will be disabled to block the unauthorized device.

2. Q: How do I update the MAC address table if a device's MAC changes?
A: The MAC address table automatically updates; you don't need to manually change entries. However, you need to update the static entries to reflect the new permitted MAC addresses.

3. Q: Can I use port security with VLANs?
A: Yes, you can. Combining port security with VLANs further isolates authorized devices and controls their network access.

4. Q: What's the difference between `switchport port-security violation restrict` and `shutdown`?
A: `restrict` prevents the unauthorized device from connecting and logs the event, while `shutdown` disables the port, effectively blocking all communication.

5. Q: How can I recover a port if it's shut down due to a port security violation?
A: Find the culprit and reset the port on the switch or configure the correct MAC addresses for the authorized device.

This guide provides a robust framework for implementing port security on your network. Remember to adapt the commands and configurations to match your specific network needs.

Unlocking Network Security: Mastering Port Security with Packet Tracer 11.1.10

Are your network connections vulnerable to unauthorized access? Imagine a malicious actor gaining entry through a seemingly innocuous port, crippling your entire network infrastructure. This isn't science fiction; it's a very real threat in today's interconnected world. Fortunately, you have the power to fortify your defenses, and Packet Tracer 11.1.10 provides the crucial tools to implement port security effectively. This comprehensive guide will equip you with the knowledge and practical skills to secure your network against threats.

Understanding the Importance of Port Security

Every network interface card (NIC) on your network is essentially a doorway. Unsecured ports are like leaving the front door unlocked – anyone can walk right in. Port security, a vital network security mechanism, helps control access to these ports by restricting the allowed devices that can connect. This dramatically reduces the risk of unauthorized access, malicious attacks, and data breaches.

Why is Port Security Necessary?

Defense against unauthorized access: Prevents rogue devices from connecting to the network.
Protection against MAC address spoofing: Ensures only legitimate devices can access the port.
Minimizes the risk of denial-of-service (DoS) attacks: Helps safeguard the network from malicious attempts to overwhelm it.
Reduced vulnerability to man-in-the-middle (MITM) attacks: Hinders attackers' ability to intercept network traffic.
Improved overall network security posture: Creates a stronger, more secure network environment.

The Growing Threat Landscape

The complexity and sophistication of cyber threats are constantly evolving. Attack vectors are becoming more varied and targeted, with malicious actors exploring every avenue to gain access to valuable information. According to recent reports, the average cost of a data breach is exceeding $4.24 million. This necessitates proactive measures like port security to safeguard your network.

Implementing Port Security with Packet Tracer 11.1.10

Packet Tracer 11.1.10 offers a highly effective simulated environment for learning and

implementing various network security concepts, including port security. This interactive platform allows you to experiment with different configurations and scenarios, enhancing your understanding and practical skills.

Key Concepts in Implementing Port Security

Understanding the core concepts is crucial for success. These concepts include:

MAC Address Filtering: Defining a whitelist of allowed MAC addresses for each port.
Violation Mode: Choosing how the switch responds to an unauthorized MAC address (e.g., shutdown the port).
Security Violation Count: Keeping track of MAC address attempts and providing detailed logging to help with troubleshooting.
Static MAC Address: Assigning a specific MAC address for each connected device.
Dynamic Updates: Manually updating the port's MAC address table.

Practical Application & Example

Let's say you have a network with three devices: a router, a server, and a workstation. Using Packet Tracer, you can configure port security on the switch connecting these devices. You would add the MAC addresses of the router, server, and workstation to the switch's configuration. If a device with a different MAC address attempts to connect, the switch can be configured to immediately shut down the port, alerting network administrators. This prevents unauthorized access and minimizes the risk of a potential breach.

Benefits of using Packet Tracer 11.1.10 for Port Security Implementation

Interactive learning: Hands-on simulations ensure a practical understanding.
Risk-free experimentation: Safely test different configurations without impacting live networks.
Gradual learning curve: Step-by-step instructions help even beginners master the concepts.
Comprehensive coverage: Provides a deep understanding of port security principles.
Development of critical troubleshooting skills: Identifying and resolving configuration errors.

Troubleshooting Common Issues

One common issue is incorrect configuration. Packet Tracer's simulation environment allows for detailed debugging, helping to pinpoint the source of errors and resolve them efficiently.

Advanced Considerations

Advanced Port Security Techniques

Using VLANs with Port Security: Isolate problematic ports to contain the impact of security breaches.
Implementing Port Security on Wireless Networks: Protecting access points against unauthorized devices.
Integrating with Network Management Systems (NMS): Centralized monitoring and management for easier troubleshooting and response.

Conclusion: Taking Action Towards a Secure Network

Implementing port security is a proactive measure that strengthens network defenses against ever-increasing cyber threats. By utilizing Packet Tracer 11.1.10, you can acquire the skills and confidence to protect your network infrastructure. Empower yourself with knowledge and experience – begin implementing port security today to build a safer network environment for your organization.

Advanced FAQs

1. Can port security be implemented on a single port or the entire network at once? You can apply port security to individual ports on a switch, or a combination of them.
2. How does port security affect network performance? Properly configured, port security impacts network performance minimally.
3. How do you handle dynamic IP addresses with port security? Dynamic IP addresses can be handled by configuring the switch to accept changes in MAC addresses dynamically.
4. Are there any limitations to port security? Port security may not always detect sophisticated spoofing techniques and requires periodic MAC address updates.
5. What role does port security play in mitigating network vulnerabilities? Port security is a crucial defense against a variety of potential network vulnerabilities by restricting unauthorized access at the port level.

How do I know which eBook platform is the best for me? Finding the best eBook platform depends on your reading preferences and device compatibility. Research different platforms, read user reviews, and explore their features before making a choice. Are free eBooks of good quality? Yes, many reputable platforms offer high-quality free eBooks, including classics and public domain works. However, make sure to verify the source to ensure the eBook credibility. Can I read eBooks without an eReader? Absolutely! Most eBook platforms offer web-based readers or mobile apps that allow you to read eBooks on your computer, tablet, or smartphone. How do I avoid digital eye strain while reading eBooks? To prevent digital eye strain, take regular breaks, adjust the font size and background color, and ensure proper lighting while reading eBooks. What the advantage of interactive eBooks? Interactive eBooks incorporate multimedia elements, quizzes, and activities, enhancing the reader engagement and providing a more immersive learning experience. 11110 Packet Tracer Implement Port Security is one of the best book in our library for free trial. We provide copy of 11110 Packet Tracer Implement Port Security in digital format, so the resources that you find are reliable. There are also many Ebooks of related with 11110 Packet Tracer Implement Port Security. Where to download 11110 Packet Tracer Implement Port Security online for free? Are you looking for 11110 Packet Tracer Implement Port Security PDF? This is definitely going to save you time and cash in something you should think about.

In this digital age, the convenience of accessing information at our fingertips has become a necessity. Whether its research papers, eBooks, or user manuals, PDF files have become the preferred format for sharing and reading documents. However, the cost associated with purchasing PDF files can sometimes be a barrier for many individuals and organizations. Thankfully, there are numerous websites and platforms that allow users to download free PDF files legally. In this article, we will explore some of the best platforms to download free PDFs. One of the most popular platforms to download free PDF files is Project Gutenberg. This online library offers over 60,000 free eBooks that are in the public domain. From classic literature to historical documents, Project Gutenberg provides a wide range of

PDF files that can be downloaded and enjoyed on various devices. The website is user-friendly and allows users to search for specific titles or browse through different categories. Another reliable platform for downloading 11110 Packet Tracer Implement Port Security free PDF files is Open Library. With its vast collection of over 1 million eBooks, Open Library has something for every reader. The website offers a seamless experience by providing options to borrow or download PDF files. Users simply need to create a free account to access this treasure trove of knowledge. Open Library also allows users to contribute by uploading and sharing their own PDF files, making it a collaborative platform for book enthusiasts. For those interested in academic resources, there are websites dedicated to providing free PDFs of research papers and scientific articles. One such website is Academia.edu, which allows researchers and scholars to share their work with a global audience. Users can download PDF files of research papers, theses, and dissertations covering a wide range of subjects. Academia.edu also provides a platform for discussions and networking within the academic community. When it comes to downloading 11110 Packet Tracer Implement Port Security free PDF files of magazines, brochures, and catalogs, Issuu is a popular choice. This digital publishing platform hosts a vast collection of publications from around the world. Users can search for specific titles or explore various categories and genres. Issuu offers a seamless reading experience with its user-friendly interface and allows users to download PDF files for offline reading. Apart from dedicated platforms, search engines also play a crucial role in finding free PDF files. Google, for instance, has an advanced search feature that allows users to filter results by file type. By specifying the file type as "PDF," users can find websites that offer free PDF downloads on a specific topic. While downloading 11110 Packet Tracer Implement Port Security free PDF files is convenient, its important to note that copyright laws must be respected. Always ensure that the PDF files you download are legally available for free. Many authors and publishers voluntarily provide free PDF versions of their work, but its essential to be cautious and verify the authenticity of the source before downloading 11110 Packet Tracer Implement Port Security. In conclusion, the internet offers numerous platforms and websites that allow users to download free PDF files legally. Whether its classic literature, research papers, or magazines, there is something for everyone. The platforms mentioned in this article, such as Project Gutenberg, Open Library, Academia.edu, and Issuu, provide access to a vast collection of PDF files. However, users should always be cautious and verify the legality of the source before downloading 11110 Packet Tracer Implement Port Security any PDF files. With these platforms, the world of PDF downloads is just a click away.

1978

2012-12-06 This volume constitutes the proceedings of the Produced Water Seminar held in Trondheim, Norway, in September 1995. Hosted by Statoil Research and Development and IKU Petroleum Research, the seminar was an update of the 1992 seminar of the same title held in San Diego, California (Ray and Engelhardt, 1992). Produced water remains the largest volume waste stream from oil and gas production offshore. In the North and Norwegian Seas, produced water volumes are projected to increase significantly over the coming decades, as oil reservoirs near depletion. These releases are therefore the focus of continuing environmental concern. The purpose of this seminar was to provide a forum for scientists, legislators, and industrial and environmental representatives to share recent information and research results, and to encourage cooperative pursuit of solutions in the future. The success of the seminar, and the quality of this volume, are due in large part to the many authors from around the world who presented almost 50 posters and papers focused on environmental issues and mitigation technologies. In addition, we wish to acknowledge the contributions of the local and international organizing committees. Local Committee Asbj0fg 0verli and Heidi Torp, Statoil Egil Wanvik and Laila S. Olden, IKU Petroleum Research International Committee James P. Ray, Shell Chemical and Petroleum Products Companies Alexis E. Steen, American Petroleum Institute Theodor C. Sauer, Battelle Ocean Sciences Steven A. Flynn, British Petroleum Martin C. Th. Scholten, TNO Kjell Lohne, Statoil Ingvild Martinsen, Norwegian Pollution Control Authority. This volume constitutes the proceedings of the Produced Water Seminar held in Trondheim Norway in September 1995

1981

2017-11-01 This valuable reference delineates the ground water quality concerns associated with the planning and usage of septic tank systems. Septic tank systems represent a significant source of ground water pollution in the United States. Since many existing systems are exceeding their design life by several-fold, the usage of synthetic organic chemicals in the household and for system cleaning is increasing, and larger-scale systems are being designed and used. This valuable reference delineates the ground water quality concerns associated with the planning and usage of septic tank systems

2012-12-06 The International Conference on the State of the Art on Biogas Technology, Transfer and Diffusion was held in Cairo, Egypt, from 17 to 24 November 1984. The Conference was organized by the Egyptian Academy of Scientific Research and Technology (ASR T), the Egyptian National Research Centre (NRC), the Bioenergy Systems and Technology project (BST) of the US Agency for International Development (US/AID) Office of Energy, and the National Academy of Sciences (NAS). A number of

international organizations and agencies co-sponsored the Conference. More than 100 participants from 40 countries attended. The purpose of the Conference was to assess the viability of biogas technology (BGT) and propose future courses of action for exploiting BGT prospects to the fullest extent. The Conference emphasized a balanced coverage of technical, environ mental, social, economic and organizational aspects relevant to biogas systems design, operation and diffusion. It was organized to incorporate experiences that are pertinent, for the most part, to developing countries. In addition to the wide spectrum of presentations and country programs, structured and non-structured discussions among the participants were strongly encouraged in thematic sessions at round-table discussions, and through personal contacts during poster sessions and field trips. It was clear from the enthusiastic response of most participants that the Conference, in large measure, succeeded in fulfilling its mission. Although draft papers were distributed to all participants, it was felt that the results obtained were worthy of organized and refined documentation. And this is precisely what this book intends to do. Although draft papers were distributed to all participants it was felt that the results obtained were worthy of organized and refined documentation And this is precisely what this book intends to do

1984

2002-03-14 The #1 menace for computer systems worldwide, network hacking can result in mysterious server crashes, data loss, and other problems that are not only costly to fix but difficult to recognize. Author John Chirillo knows how these can be prevented, and in this book he brings to the table the perspective of someone who has been invited to break into the networks of many Fortune 1000 companies in order to evaluate their security policies and conduct security audits. He gets inside every detail of the hacker's world, including how hackers exploit security holes in private and public networks and how network hacking tools work. As a huge value-add, the author is including the first release of a powerful software hack attack tool that can be configured to meet individual customer needs. In this highly provocative work youll discover The hackers perspective on networking protocols and communication technologies A complete hackers technology handbook illustrating techniques used by hackers crackers phreaks and

2003 Now there is a comprehensive reference to provide tools on implementing an energy audit for any type of facility. Containing forms, checklists and handy working aids, this book is for anyone implementing an energy audit. Accounting procedures, rate of return, analysis and software programs are included to provide evaluation tools for audit recommendations. Technologies for electrical, mechanical and building systems are covered in detail. Now there is a comprehensive reference to

provide tools on implementing an energy audit for any type of facility Containing forms checklists and handy working aids this book is for anyone implementing an energy audit

1987

2001-09-07 CD-ROM contains: 10,000 pages containing the full texts, tools, and exploits described and previewed in the book. This book delves into the underground of hacking to offer a detailed look at the program files and code snippets used to get into companies

2008 'Network Fundamentals' is a complete collection of the exercises specifically written for the CCNA Exploration course in the Cisco Networking Academy Program. The book is designed to give students practice exercises and hands-on labs to study the course concepts in-depth. The book is designed to give students practice exercises and hands on labs to study the course concepts in depth

1996

1995 The fifth edition of this very successful IBM Redbook provides a complete understanding of the TCP/IP protocol suite and how IBM's suite of networking products work in a heterogeneous networking environment. New features include an Internet access chapter, and new sections on MIME, SNMPv2, DHCP, and other state-of-the-art protocols. The fifth edition of this very successful IBM Redbook provides a complete understanding of the TCP IP protocol suite and how IBMs suite of networking products work in a heterogeneous networking environment

2019-02-08 Embedded System Interfacing: Design for the Internet-of-Things (IoT) and Cyber-Physical Systems (CPS) takes a comprehensive approach to the interface between embedded systems and software. It provides the principles needed to understand how digital and analog interfaces work and how to design new interfaces for specific applications. The presentation is self-contained and practical, with discussions based on real-world components. Design examples are used throughout the book to illustrate important concepts. This book is a complement to the author's Computers as Components, now in its fourth edition, which concentrates on software running on the CPU, while Embedded System Interfacing explains the hardware surrounding the CPU. - Provides a comprehensive background in embedded system interfacing techniques - Includes design examples to illustrate important concepts and serve as the basis for new designs - Discusses well-known, widely available hardware components and computer-aided design tools This book is a complement to the authors Computers as Components now in its fourth edition which concentrates on software running on the CPU while Embedded System Interfacing explains the hardware surrounding the CPU

1975

1989 This proceedings contains 16 papers on recreation and adventure programming, outdoor education, and outdoor leadership training. The papers are:

(1) Beyond Recreation: Our Classroom Is Wild America (Barry Auskern); (2) Outward Bound Leadership Model: An Exploratory Study of Leadership Variables (Natalie L. Bartley); (3) 'Putting a Little Flavor in Your Outings!' Getting to Know the World of Edible and Useful Wild Plants (Charles Chase); (4) Risk Management in High Adventure Outdoor Pursuits (Jerry Cinnamon); (5) The Identification and Modification of Situational Fears Associated with Outdoor Recreation (Alan Ewert); (6) Outdoor Programming in the Southern United States (Jim Gilbert and Wayne Taylor); (7) Winter Wilderness Travel and Camping (Norman Gilchrest); (8)Environmental Activism, Public Education and Outdoor Programming: A Union of Necessity (Terry Hartig and Peter Bowler); (9) Technical Tree Climbing (Peter Jenkins); (10) Leadership: The Development of Self Concept (Rick Matishak and Lyle Benson); (11) Survey Compilation: Status and Concerns of the Outdoor Recreation Profession (Rodney K. Neubert and Julian A. McPhee); (12) Freshman Wilderness Orientation Programs: Model Programs across the Country (Marty O'Keefe); (13) Eagle Mount--Montana's Premiere Handicapped Outdoor Recreation Program (Curt Shirer); (14) Successfully Adapting Financially Subsidized Outdoor Programs to 'Pay Their Own Way' Programs (Alf Skrastins); (15) Passages: Helping College Students Matriculate through Outdoor Adventure (Bob Stremba); and (16) How To Successfully Change from a Financially Subsidized Outdoor Program to a Pays-Its-Own-Way Outdoor Program (David J. Webb). Appendices include descriptions of conference presentations and events, a list of conference participants, and biographical information on presenters. (KS) This proceedings contains 16 papers on recreation and adventure programming outdoor education and outdoor leadership training

2015

1963 Includes reports by the U.S. Dept. of Labor (called 1963- : Manpower requirements, resources, utilization and training), and the U.S. Dept. of Health, Education, and Welfare , 1975- Includes reports by the U S Dept of Labor called 1963 Manpower requirements resources utilization and training and the U S Dept of Health Education and Welfare 1975

1982 Since the complexity of police services does not lend itself to standardized performance measures, measurement techniques should be designed to inform more about what police do and how they affect their communities. This report reviews conventional police measurement practices and offers ways to improve the management value of performance information. Traditional performance measurement has emphasized the measurement of individual departments' effectiveness in preventing crime. This approach fails to consider the broad range of other police duties, citizens' expectations of police, and how police activities produce

social change. Police can be evaluated in terms of efficiency, effectiveness, equity, and accountability, but citizens disagree about which of these performance criteria are the most important because community/police problems are too diverse. Instead of developing uniform, inflexible performance standards to apply globally to entire departments, evaluators should ask more detailed questions about common police processes and their results. Sketchy knowledge of how policing works now produces many hypotheses, but rarely standards worthy of emulation. Evaluators should develop better theories about police functions, obtain more reliable data, and control data collection costs with the aid of police managers so that measures inform departmental policymakers. Tables, diagrams, and 197 references are given. Appendixes include police services study data and a list of problem codes. This report reviews conventional police measurement practices and offers ways to improve the management value of performance information

2017-04-18 Are you looking to pass the coveted Cisco CCNA Routing and Switching exam? There are so many study guides to choose from, but most of them only serve to confuse students with unnecessary technical jargon and useless information rather than teach them what they need to know to pass the exam and actually apply what they have learned to the real world of IT. This book will prepare you for the latest Cisco CCNA Routing exams, including: - 200-125 CCNA - Interconnecting Cisco Networking Devices: Accelerated (CCNAX) - 100-105 ICND1 - Interconnecting Cisco Networking Devices: Part 1 (ICND1) - 200-105 ICND2 - Interconnecting Cisco Networking Devices: Part 2 (ICND2) Over 50% of the CCNA exam marks are awarded for completing the notoriously difficult practical lab scenarios, so why are there next to no labs to be found in most CCNA study guides? We've packed over 45 follow-along mini-labs and 32 full labs into this study guide, as well as solutions and configurations you can try at home so that you really learn how to configure and troubleshoot all the important exam topics, including: - Routing protocols such as EIGRP, OSPF and BGP - IPv6 internetworking - Securing the router and switch with passwords - VLANs and VLAN security - Access lists and Network Address Translation - Backing up important configuration files - Planning and designing a network addressing scheme - Spanning Tree Protocol - Answering any subnetting question within seconds - guaranteed! - Quickly troubleshooting and fixing network faults in the exam and in the real world - Setting up a router and switch from scratch with no previous experience - And much more The book has been broken down into ICND1 topics in the first half and ICND2 topics in the second half so that you can take either the one-exam or two-exam route. In their day jobs the authors work on live enterprise networks for global companies, so let them

share their decades of internetworking experience with you. They have packed this study guide with exam tips and real-world advice that you can use on the job to avoid common mistakes made by both junior and experienced network engineers. These mistakes can cost you your job. As well as the labs and mini-labs, the theory has been broken up into easy to manage modules so that you can study at your own pace and really master the technologies. There is more than $400 worth of practice exams, advanced challenge labs, and study videos at the URL below for you to enjoy free of charge and to guarantee your success come exam day. https://www.howtonetwork.com/ccnasimplified

There are so many study guides to choose from but most of them only serve to confuse students with unnecessary technical jargon and useless information rather than teach them what they need to know to pass the exam and actually apply what