Software Defined Networking Done Right

The book is devoted to the selected resource allocation problems in Software- Defined Networks. Moreover, it covers results concerning Software Defined Wide Area Networks (SD-WANs) which is one of the current networking hot topics. The variety of different cases is considered including virtualization and information-centric paradigm. For each case, the mathematical model together with the problem formulation is given and some solution algorithms are proposed. The algorithms are discussed and evaluated, mostly with simulations.
The advancement of technology is a standard of modern daily life, whether it be the release of a new cellphone, computer, or a self-driving car. Due to this constant advancement, the networks on which these technologies operate must advance as well. Innovations in Software-Defined Networking and Network Functions Virtualization is a critical scholarly publication that observes the advances made in network infrastructure through achieving cost efficacy while maintaining maximum flexibility for the formation and operation of these networks. Featuring coverage on a broad selection of topics, such as software-defined storage, openflow controller, and storage virtualization, this publication is geared toward professionals, computer engineers, academicians, students, and researchers seeking current and relevant research on the advancements made to network infrastructures.
Written by two experts in the field who deal with QOS predicaments every day and now in this 2nd edition give special attention to the realm of Data Centers, em style="mso-bidi-font-style: normal;"QoS Enabled Networks:Tools and Foundations, 2nd Edition provides a lucid understanding of modern QOS theory mechanisms in packet networks and how to apply them in practice. This book is focuses on the tools and foundations of QoS providing the knowledge to understand what benefits QOS offers and what can be built on top of it.
This SpringerBrief provides essential insights on the SDN application designing and deployment in distributed datacenters. In this book, three key problems are discussed: SDN application designing, SDN deployment and SDN management. This book demonstrates how to design the SDN-based request allocation application in distributed datacenters. It also presents solutions for SDN controller placement to deploy SDN in distributed datacenters. Finally, an SDN management system is proposed to guarantee the performance of datacenter networks which are covered and controlled by many heterogeneous controllers. Researchers and practitioners alike will find this book a valuable resource for further study on Software Defined Networking.
Software Defined Networking: Design and Deployment provides a comprehensive treatment of software defined networking (SDN) suitable for new network managers and experienced network professionals. Presenting SDN in context with more familiar network services and challenges, this accessible text: Explains the importance of virtualization, particularly the impact of virtualization on servers and networks Addresses SDN, with an emphasis on the network control plane Discusses SDN implementation and the impact on service providers, legacy networks, and network vendors Contains a case study on Google’s initial implementation of SDN Investigates OpenFlow, the hand-in-glove partner of SDN Looks forward toward more programmable networks and the languages needed to manage these environments Software Defined Networking: Design and Deployment offers a unique perspective of the business case and technology motivations for considering SDN solutions. By identifying the impact of SDN on traffic management and the potential for network service growth, this book instills the knowledge needed to manage current and future demand and provisioning for SDN.
This updated study guide by two security experts will help you prepare for the CompTIA CySA+ certification exam. Position yourself for success with coverage of crucial security topics! Where can you find 100% coverage of the revised CompTIA Cybersecurity Analyst+ (CySA+) exam objectives? It’s all in the CompTIA CySA+ Study Guide Exam CS0-002, Second Edition! This guide provides clear and concise information on crucial security topics. You’ll be able to gain insight from practical, real-world examples, plus chapter reviews and exam highlights. Turn to this comprehensive resource to gain authoritative coverage of a range of security subject areas. Review threat and vulnerability management topics Expand your knowledge of software and systems security Gain greater understanding of security operations and monitoring Study incident response information Get guidance on compliance and assessment The CompTIA CySA+ Study Guide, Second Edition connects you to useful study tools that help you prepare for the exam. Gain confidence by using its interactive online test bank with hundreds of bonus practice questions, electronic flashcards, and a searchable glossary of key cybersecurity terms. You also get access to hands-on labs and have the opportunity to create a cybersecurity toolkit. Leading security experts, Mike Chapple and David Seidl, wrote this valuable guide to help you prepare to be CompTIA Security+ certified. If you’re an IT professional who has earned your CompTIA Security+ certification, success on the CySA+ (Cybersecurity Analyst) exam stands as an impressive addition to your professional credentials. Preparing and taking the CS0-002exam can also help you plan for advanced certifications, such as the CompTIA Advanced Security Practitioner (CASP+).
Despite the explosion of networking services and applications in the past decades, the basic technological underpinnings of the Internet have remained largely unchanged. At its heart are special-purpose appliances that connect us to the digital world, commonly known as switches and routers. Now, however, the traditional framework is being increasingly challenged by new methods that are jostling for a position in the “next-generation” Internet. The concept of a network that is becoming more programmable is one of the aspects that are taking center stage. This opens new possibilities to embed software applications inside the network itself and to manage networks and communications services with unprecedented ease and efficiency. In this edited volume, distinguished experts take the reader on a tour of different facets of programmable network infrastructure and applications that exploit it. Presenting the state of the art in network embedded management and applications and programmable network infrastructure, the book conveys fundamental concepts and provides a glimpse into various facets of the latest technology in the field.
This book describes the concept of a Software Defined Mobile Network (SDMN), which will impact the network architecture of current LTE (3GPP) networks. SDN will also open up new opportunities for traffic, resource and mobility management, as well as impose new challenges on network security. Therefore, the book addresses the main affected areas such as traffic, resource and mobility management, virtualized traffics transportation, network management, network security and techno economic concepts. Moreover, a complete introduction to SDN and SDMN concepts. Furthermore, the reader will be introduced to cutting-edge knowledge in areas such as network virtualization, as well as SDN concepts relevant to next generation mobile networks. Finally, by the end of the book the reader will be familiar with the feasibility and opportunities of SDMN concepts, and will be able to evaluate the limits of performance and scalability of these new technologies while applying them to mobile broadb and networks.
Software Defined NetworkingDesign and DeploymentCRC Press
Network infrastructures are growing rapidly to meet the needs of business, but the required repolicing and reconfiguration provide challenges that need to be addressed. The software-defined network (SDN) is the future generation of Internet technology that can help meet these challenges of network management. This book includes quantitative research, case studies, conceptual papers, model papers, review papers, and theoretical backing on SDN. This book investigates areas where SDN can help other emerging technologies deliver more efficient services, such as IoT, industrial IoT, NFV, big data, blockchain, cloud computing, and edge computing. The book demonstrates the many benefits of SDNs, such as reduced costs, ease of deployment and management, better scalability, availability, flexibility and fine-grained control of traffic, and security. The book demonstrates the many benefits of SDN, such as reduced costs, ease of deployment and management, better scalability, availability, flexibility and fine-grained

control of traffic, and security. Chapters in the volume address: Design considerations for security issues and detection methods State-of-the-art approaches for mitigating DDos attacks using SDN Big data using Apache Hadoop for processing and analyzing large amounts of data Different tools used for attack simulation Network policies and policy management approaches that are widely used in the context of SDN Dynamic flow tables, or static flow table management A new four-tiered architecture that includes cloud, SDN-controller, and fog computing Architecture for keeping computing resources available near the industrial IoT network through edge computing The impact of SDN as an innovative approach for smart city development More. The book will be a valuable resource for SDN researchers as well as academicians, research scholars, and students in the related areas.

This book presents a range of cloud computing security challenges and promising solution paths. The first two chapters focus on practical considerations of cloud computing. In Chapter 1, Chandramouli, Iorga, and Chokani describe the evolution of cloud computing and the current state of practice, followed by the challenges of cryptographic key management in the cloud. In Chapter 2, Chen and Sion present a dollar cost model of cloud computing and explore the economic viability of cloud computing with and without security mechanisms involving cryptographic mechanisms. The next two chapters address security issues of the cloud infrastructure. In Chapter 3, Szefer and Lee describe a hardware-enhanced security architecture that protects the confidentiality and integrity of a virtual machine's memory from an untrusted or malicious hypervisor. In Chapter 4, Tsugawa et al. discuss the security issues introduced when Software-Defined Networking (SDN) is deployed within and across clouds. Chapters 5-9 focus on the protection of data stored in the cloud. In Chapter 5, Wang et al. present two storage isolation schemes that enable cloud users with high security requirements to verify that their disk storage is isolated from some or all other users, without any cooperation from cloud service providers. In Chapter 6, De Capitani di Vimercati, Foresti, and Samarati describe emerging approaches for protecting data stored externally and for enforcing fine-grained and selective accesses on them, and illustrate how the combination of these approaches can introduce new privacy risks. In Chapter 7, Le, Kant, and Jajodia explore data access challenges in collaborative enterprise computing environments where multiple parties formulate their own authorization rules, and discuss the problems of rule consistency, enforcement, and dynamic updates. In Chapter 8, Smith et al. address key challenges to the practical realization of a system that supports query execution over remote encrypted data without exposing decryption keys or plaintext at the server. In Chapter 9, Sun et al. provide an overview of secure search techniques over encrypted data, and then elaborate on a scheme that can achieve privacy-preserving multi-keyword text search. The next three chapters focus on the secure deployment of computations to the cloud. In Chapter 10, Oktay el al. present a risk-based approach for workload partitioning in hybrid clouds that selectively outsources data and computation based on their level of sensitivity. The chapter also describes a vulnerability assessment framework for cloud computing environments. In Chapter 11, Albanese et al. present a solution for deploying a mission in the cloud while minimizing the mission's exposure to known vulnerabilities, and a cost-effective approach to harden the computational resources selected to support the mission. In Chapter 12, Kontaxis et al. describe a system that generates computational decoys to introduce uncertainty and deceive adversaries as to which data and computation is legitimate. The last section of the book addresses issues related to security monitoring and system resilience. In Chapter 13, Zhou presents a secure, provenance-based capability that captures dependencies between system states, tracks state changes over time, and that answers attribution questions about the existence, or change, of a system's state at a given time. In Chapter 14, Wu et al. present a monitoring capability for multicore architectures that runs monitoring threads concurrently with user or kernel code to constantly check for security violations. Finally, in Chapter 15, Hasan Cam describes how to manage the risk and resilience of cyber-physical systems by employing controllability and observability techniques for linear and non-linear systems.

The implementation of cloud technologies in healthcare is paving the way to more effective patient care and management for medical professionals around the world. As more facilities start to integrate cloud computing into their healthcare systems, it is imperative to examine the emergent trends and innovations in the field. Cloud Computing Systems and Applications in Healthcare features innovative research on the impact that cloud technology has on patient care, disease management, and the efficiency of various medical systems. Highlighting the challenges and difficulties in implementing cloud technology into the healthcare field, this publication is a critical reference source for academicians, technology designers, engineers, professionals, analysts, and graduate students.

How does network virtualization contrast to Software Defined Networking (SDN)? How is the scalability? What abstractions do you have in networking? What role do abstractions play in networking? What are the scaling limits of the current design? Defining, designing, creating, and implementing a process to solve a challenge or meet an objective is the most valuable role... In EVERY group, company, organization and department. Unless you are talking a one-time, single-use project, there should be a process. Whether that process is managed and implemented by humans, AI, or a combination of the two, it needs to be designed by someone with a complex enough perspective to ask the right questions. Someone capable of asking the right questions and step back and say, 'What are we really trying to accomplish here? And is there a different way to look at it?' This Self-Assessment empowers people to do just that - whether their title is entrepreneur, manager, consultant, (Vice-)President, CxO etc... - they are the people who rule the future. They are the person who asks the right questions to make Software Defined Network investments work better. This Software Defined Network All-Inclusive Self-Assessment enables You to be that person. All the tools you need to an in-depth Software Defined Network Self-Assessment. Featuring 954 new and updated case-based questions, organized into seven core areas of process design, this Self-Assessment will help you identify areas in which Software Defined Network improvements can be made. In using the questions you will be better able to: - diagnose Software Defined Network projects, initiatives, organizations, businesses and processes using accepted diagnostic standards and practices - implement evidence-based best practice strategies aligned with overall goals - integrate recent advances in Software Defined Network and process design strategies into practice according to best practice guidelines Using a Self-Assessment tool known as the Software Defined Network Scorecard, you will develop a clear picture of which Software Defined Network areas need attention. Your purchase includes access details to the Software Defined Network self-assessment dashboard download which gives you your dynamically prioritized projects-ready tool and shows your organization exactly what to do next. You will receive the following contents with New and Updated specific criteria: - The latest quick edition of the book in PDF - The latest complete edition of the book in PDF, which criteria correspond to the criteria in... - The Self-Assessment Excel Dashboard - Example pre-filled Self-Assessment Excel Dashboard to get familiar with results generation - In-depth and specific Software Defined Network Checklists - Project management checklists and templates to assist with implementation INCLUDES LIFETIME SELF ASSESSMENT UPDATES Every self assessment comes with Lifetime Updates and Lifetime Free Updated Books. Lifetime Updates is an industry-first

feature which allows you to receive verified self assessment updates, ensuring you always have the most accurate information at your fingertips.

This book provides a quick reference and insights into modeling and optimization of software-defined networks (SDNs). It covers various algorithms and approaches that have been developed for optimizations related to the control plane, the considerable research related to data plane optimization, and topics that have significant potential for research and advances to the state-of-the-art in SDN. Over the past ten years, network programmability has transitioned from research concepts to more mainstream technology through the advent of technologies amenable to programmability such as service chaining, virtual network functions, and programmability of the data plane. However, the rapid development in SDN technologies has been the key driver behind its evolution. The logically centralized abstraction of network states enabled by SDN facilitates programmability and use of sophisticated optimization and control algorithms for enhancing network performance, policy management, and security.Furthermore, the centralized aggregation of network telemetry facilitates use of data-driven machine learning-based methods. To fully unleash the power of this new SDN paradigm, though, various architectural design, deployment, and operations questions need to be addressed. Associated with these are various modeling, resource allocation, and optimization opportunities.The book covers these opportunities and associated challenges, which represent a ``call to arms'' for the SDN community to develop new modeling and optimization methods that will complement or improve on the current norms.

This practical text/reference provides an exhaustive guide to setting up and sustaining software-defined data centers (SDDCs). Each of the core elements and underlying technologies are explained in detail, often supported by real-world examples. The text illustrates how cloud integration, brokerage, and orchestration can ensure optimal performance and usage of data resources, and what steps are required to secure each component in a SDDC. The coverage also includes material on hybrid cloud concepts, cloud-based data analytics, cloud configuration, enterprise DevOps and code deployment tools, and cloud software engineering. Topics and features: highlights how technologies relating to cloud computing, IoT, blockchain, and AI are revolutionizing business transactions, operations, and analytics; introduces the concept of Cloud 2.0, in which software-defined computing, storage, and networking are applied to produce next-generation cloud centers; examines software-defined storage for storage virtualization, covering issues of cloud storage, storage tiering, and deduplication; discusses software-defined networking for network virtualization, focusing on techniques for network optimization in data centers; reviews the qualities and benefits of hybrid clouds, that bridge private and public cloud environments; investigates the security management of a software-defined data center, and proposes a framework for managing hybrid IT infrastructure components; describes the management of multi-cloud environments through automated tools, and cloud brokers that aim to simplify cloud access, use and composition; covers cloud orchestration for automating application integration, testing, infrastructure provisioning, software deployment, configuration, and delivery. This comprehensive work is an essential reference for all practitioners involved with software-defined data center technologies, hybrid clouds, cloud service management, cloud-based analytics, and cloud-based software engineering.

For more than 20 years, Network World has been the premier provider of information, intelligence and insight for network and IT executives responsible for the digital nervous systems of large organizations. Readers are responsible for designing, implementing and managing the voice, data and video systems their companies use to support everything from business critical applications to employee collaboration and electronic commerce.

Ultimate coverage and hands-on practice for the second MCSA Windows Server 2016 exam MCSA Windows Server 2016 Study Guide: Exam 70-741 offers complete preparation for the second exam in the MCSA series. With comprehensive coverage of all exam objectives led by a four-time Microsoft MVP winner, this book is your ideal companion for thorough preparation. Optimize your study time with hundreds of practice questions that pinpoint your weak spots, and try your hand at real-world application with exercises that reflect the MCSA skill set. Access to the Sybex interactive online practice test environment provides electronic flashcards, a glossary, practice exams and more, so you can study anywhere, any time; this invaluable study guide goes beyond mere review to help you enter the exam with full confidence in your abilities. The Microsoft Certified Solutions Associate certification puts your skills in demand—but first you must pass a series of three exams; exam 70-741 is the second step, testing your Windows 2016 networking knowledge and skills. This book covers everything you need to know, giving you the exam-day advantage of comprehensive prep. Master 100 percent of the exam objective domains Learn how these skills are applied in real-world scenarios Solidify your understanding with hands-on exercises Access electronic flashcards, practice exams, and more! How well do you deploy, manage, and maintain a server? Can you expertly configure file and print servers, network access and services, and network policy server infrastructure? Have you configured and managed Active Directory and Group Policy? Don't leave anything to chance—MCSA Windows Server 2016 Study Guide: Exam 70-741 tells you all you need to know to pass with flying colors.

This book introduces the software defined system concept, architecture, and its enabling technologies such as software defined sensor networks (SDSN), software defined radio, cloud/fog radio access networks (C/F-RAN), software defined networking (SDN), network function virtualization (NFV), software defined storage, virtualization and docker. The authors also discuss the resource allocation and task scheduling in software defined system, mainly focusing on sensing, communication, networking and computation. Related case studies on SDSN, C/F-RAN, SDN, NFV are included in this book, and the authors discuss how these technologies cooperate with each other to enable cross resource management and task scheduling in software defined system. Novel resource allocation and task scheduling algorithms are introduced and evaluated. This book targets researchers, computer scientists and engineers who are interested in the information system softwarization technologies, resource allocation and optimization algorithm design, performance evaluation and analysis, next-generation communication and networking technologies, edge computing, cloud computing and IoT. Advanced level students studying these topics will benefit from this book as well.

A comprehensive collection of influential articles from one of IEEE Computer magazine’s most popular columns This book is a compendium of extended and revised publications that have appeared in the “Software Technologies” column of IEEE Computer magazine, which covers key topics in software engineering such as software development, software

correctness and related techniques, cloud computing, self-managing software and self-aware systems. Emerging properties of software technology are also discussed in this book, which will help refine the developing framework for creating the next generation of software technologies and help readers predict future developments and challenges in the field. Software Technology provides guidance on the challenges of developing software today and points readers to where the best advances are being made. Filled with one insightful article after another, the book serves to inform the conversation about the next wave of software technology advances and applications. In addition, the book: Introduces the software landscape and challenges associated with emerging technologies Covers the life cycle of software products, including concepts, requirements, development, testing, verification, evolution, and security Contains rewritten and updated articles by leaders in the software industry Covers both theoretical and practical topics Informative and thought-provoking throughout, Software Technology is a valuable book for everyone in the software engineering community that will inspire as much as it will teach all who flip through its pages.

Application Performance Management (APM) in the Digital Enterprise enables IT professionals to be more successful in managing their company’s applications. It explores the fundamentals of application management, examines how the latest technological trends impact application management, and provides best practices for responding to these changes. The recent surge in the use of containers as a way to simplify management and deploy applications has created new challenges, and the convergence of containerization, cloud, mobile, virtualization, analytics, and automation is reshaping the requirements for application management. This book serves as a guide for understanding these dramatic changes and how they impact the management of applications, showing how to create a management strategy, define the underlying processes and standards, and how to select the appropriate tools to enable management processes. Offers a complete framework for implementing effective application management using clear tips and solutions for those responsible for application management Draws upon primary research to give technologists a current understanding of the latest technologies and processes needed to more effectively manage large-scale applications Includes real-world case studies and business justifications that support application management investments

Software Defined Networks: A Comprehensive Approach, Second Edition provides in-depth coverage of the technologies collectively known as Software Defined Networking (SDN). The book shows how to explain to business decision-makers the benefits and risks in shifting parts of a network to the SDN model, when to integrate SDN technologies in a network, and how to develop or acquire SDN applications. In addition, the book emphasizes the parts of the technology that encourage opening up the network, providing treatment for alternative approaches to SDN that expand the definition of SDN as networking vendors adopt traits of SDN to their existing solutions. Since the first edition was published, the SDN market has matured, and is being gradually integrated and morphed into something more compatible with mainstream networking vendors. This book reflects these changes, with coverage of the OpenDaylight controller and its support for multiple southbound protocols, the Inclusion of NETCONF in discussions on controllers and devices, expanded coverage of NFV, and updated coverage of the latest approved version (1.5.1) of the OpenFlow specification. Contains expanded coverage of controllers Includes a new chapter on NETCONF and SDN Presents expanded coverage of SDN in optical networks Provides support materials for use in computer networking courses

The adoption of cloud and IoT technologies in both the industrial and academic communities has enabled the discovery of numerous applications and ignited countless new research opportunities. With numerous professional markets benefiting from these advancements, it is easy to forget the non-technical issues that accompany technologies like these. Despite the advantages that these systems bring, significant ethical questions and regulatory issues have become prominent areas of discussion. Social, Legal, and Ethical Implications of IoT, Cloud, and Edge Computing Technologies is a pivotal reference source that provides vital research on the non-technical repercussions of IoT technology adoption. While highlighting topics such as smart cities, environmental monitoring, and data privacy, this publication explores the regulatory and ethical risks that stem from computing technologies. This book is ideally designed for researchers, engineers, practitioners, students, academicians, developers, policymakers, scientists, and educators seeking current research on the sociological impact of cloud and IoT technologies.

This book provides readers insights into cyber maneuvering or adaptive and intelligent cyber defense. It describes the required models and security supporting functions that enable the analysis of potential threats, detection of attacks, and implementation of countermeasures while expending attacker resources and preserving user experience. This book not only presents significant education-oriented content, but uses advanced content to reveal a blueprint for helping network security professionals design and implement a secure Software-Defined Infrastructure (SDI) for cloud networking environments. These solutions are a less intrusive alternative to security countermeasures taken at the host level and offer centralized control of the distributed network. The concepts, techniques, and strategies discussed in this book are ideal for students, educators, and security practitioners looking for a clear and concise text to avant-garde cyber security installations or simply to use as a reference. Hand-on labs and lecture slides are located at http://virtualnetworksecurity.thothlab.com/. Features Discusses virtual network security concepts Considers proactive security using moving target defense Reviews attack representation models based on attack graphs and attack trees Examines service function chaining in virtual networks with security considerations Recognizes machine learning and AI in network security

This book highlights the importance of security in the design, development and deployment of systems based on Software-Defined Networking (SDN) and Network Functions Virtualization (NFV), together referred to as SDNFV. Presenting a comprehensive guide to the application of security mechanisms in the context of SDNFV, the content spans fundamental theory, practical solutions, and potential applications in future networks. Topics and features: introduces the key security challenges of SDN, NFV and Cloud Computing, providing a detailed tutorial on NFV security; discusses the

issue of trust in SDN/NFV environments, covering roots of trust services, and proposing a technique to evaluate trust by exploiting remote attestation; reviews a range of specific SDNFV security solutions, including a DDoS detection and remediation framework, and a security policy transition framework for SDN; describes the implementation of a virtual home gateway, and a project that combines dynamic security monitoring with big-data analytics to detect network-wide threats; examines the security implications of SDNFV in evolving and future networks, from network-based threats to Industry 4.0 machines, to the security requirements for 5G; investigates security in the Observe, Orient, Decide and Act (OODA) paradigm, and proposes a monitoring solution for a Named Data Networking (NDN) architecture; includes review questions in each chapter, to test the reader’s understanding of each of the key concepts described. This informative and practical volume is an essential resource for researchers interested in the potential of SDNFV systems to address a broad range of network security challenges. The work will also be of great benefit to practitioners wishing to design secure next-generation communication networks, or to develop new security-related mechanisms for SDNFV systems.
This book constitutes the thoroughly refereed post-workshop proceedings of the 21st International Workshop on Security Protocols, held in Cambridge, UK, in March 2013. The volume contains 14 revised papers with transcripts of the presentation and workshop discussion and an introduction, i.e. 15 contributions in total. The theme of the workshop was "What's Happening on the Other Channel?".
This book constitutes the revised selected papers of the 5th International Conference on Information Systems Security and Privacy, ICISSP 2019, held in Prague, Czech Republic, in February 2019. The 19 full papers presented were carefully reviewed and selected from a total of 100 submissions. The papers presented in this volume address various topical research, including new approaches for attack modelling andprevention, incident management and response, and user authentication andaccess control, as well as business and human-oriented aspects such as data pro-tection and privacy, and security awareness.
This IBM® Redbooks® publication shows how to integrate IBM Software Defined Network for Virtual Environments (IBM SDN VE) seamlessly within a new or existing data center. This book is aimed at pre- and post-sales support, targeting network administrators and other technical professionals that want to get an overview of this new and exciting technology, and see how it fits into the overall vision of a truly Software Defined Environment. It shows you all of the steps that are required to design, install, maintain, and troubleshoot the IBM SDN VE product. It also highlights specific, real-world examples that showcase the power and flexibility that IBM SDN VE has over traditional solutions with a legacy network infrastructure that is applied to virtual systems. This book assumes that you have a general familiarity with networking and virtualization. It does not assume an in-depth understanding of KVM or VMware. It is written for administrators who want to get a quick start with IBM SDN VE in their respective virtualized infrastructure, and to get some virtual machines up and running by using the rich features of the product in a short amount of time (days, not week, or months).
This book constitutes the thoroughly refereed proceedings of the 12th International Conference on e-Infrastructure and e-Services for Developing Countries, AFRICOMM 2020, held in Ebène City, Mauritius, in December 2020. Due to COVID-19 pandemic the conference was held virtually. The 20 full papers were carefully selected from 90 submissions. The papers are organized in four thematic sections on dynamic spectrum access and mesh networks; wireless sensing and 5G networks; software-defined networking; Internet of Things; e-services and big data; DNS resilience and performance. .
This best-selling guide provides a complete, practical, and thoroughly up-to-date introduction to network and computer security. COMPTIA SECURITY+ GUIDE TO NETWORK SECURITY FUNDAMENTALS, Seventh Edition, maps to the new CompTIA Security+ SY0-601 Certification Exam, providing comprehensive coverage of all domain objectives to help readers prepare for professional certification and career success. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.
Leverage the best SDN technologies for your OpenStack-based cloud infrastructure About This Book Learn how to leverage critical SDN technologies for OpenStack Networking APIs via plugins and drivers Champion the skills of achieving complete SDN with OpenStack with specific use cases and capabilities only covered in this title Discover exactly how you could implement cost-effective OpenStack SDN integration for your organization Who This Book Is For Administrators, and cloud operators who would like to implement Software Defined Networking on OpenStack clouds. Some prior experience of network infrastructure and networking concepts is assumed. What You Will Learn Understand how OVS is used for Overlay networks Get familiar with SDN Controllers with Architectural details and functionalities Create core ODL services and understand how OpenDaylight integrates with OpenStack to provide SDN capabilities Understand OpenContrail architecture and how it supports key SDN functionality such as Service Function Chaining (SFC) along with OpenStack Explore Open Network Operating System (ONOS) – a carrier grade SDN platform embraced by the biggest telecom service providers Learn about upcoming SDN technologies in OpenStack such as Dragonflow and OVN In Detail Networking is one the pillars of OpenStack and OpenStack Networking are designed to support programmability and Software-Defined Networks. OpenStack Networking has been evolving from simple APIs and functionality in Quantum to more complex capabilities in Neutron. Armed with the basic knowledge, this book will help the readers to explore popular SDN technologies, namely, OpenDaylight (ODL), OpenContrail, Open Network Operating System (ONOS) and Open Virtual Network (OVN). The first couple of chapters will provide an overview of OpenStack Networking and SDN in general. Thereafter a set of chapters are devoted to OpenDaylight (ODL), OpenContrail and their integration with OpenStack Networking. The book then introduces you to Open Network Operating System (ONOS) which is fast becoming a carrier grade SDN platform. We will conclude the book with overview of upcoming SDN projects within OpenStack namely OVN and Dragonflow. By the end of the book, the readers

will be familiar with SDN technologies and know how they can be leveraged in an OpenStack based cloud. Style and approach A hands-on practical tutorial through use cases and examples for Software Defined Networking with OpenStack.

Software-Defined Networking has been one of the most talked about topics in the field of networking in recent times. It is a new approach to designing, building and managing the configuration of network devices This report is a study on the technological landscape of this fast growing technology from an Intellectual Property (Patents) perspective.

Develop an understanding of the core principles of information systems (IS) and how these principles make a difference in today’s business environment with Stair/Reynolds' PRINCIPLES OF INFORMATION SYSTEMS, 14E. Completely reorganized for clarity and focus, this fresh new edition provides engaging new chapter opening cases and a new chapter on AI and automation. You explore the challenges and risks of cybercrime, hacking, internet of things, and artificial intelligence as you examine the latest IS research and learn from memorable examples. You can even maximize your employability as you learn how to use IS to increase profits and reduce costs in organizations while studying the latest developments in big data, business intelligence, cloud computing, e-commerce, enterprise systems, mobile computing, strategic planning, and systems development. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

This book constitutes the refereed proceedings of the 6th International Conference on E-Democracy, E-Democracy 2015, held in Athens, Greece, in December 2015. The 13 revised full papers presented together with 8 extended abstracts were carefully selected from 33 submissions. The papers are organized in topical sections on privacy in e-voting, e-polls and e-surveys; security and privacy in new computing paradigms; privacy in online social networks; e-government and e-participation; legal issues. The book also contains the extended abstracts describing progress within European research and development projects on security and privacy in the cloud; secure architectures and applications; enabling citizen-to-government communication.

The practical and conceptual knowledge you need to attain CCNP Enterprise certification From one of the most trusted study guide publishers comes CCNP Enterprise Certification Study Guide: Exam 350-401. This guide helps you develop practical knowledge and best practices for critical aspects of enterprise infrastructure so you can gain your CCNP Enterprise certification. If you’re hoping to attain a broader range of skills and a solid understanding of Cisco technology, this guide will also provide fundamental concepts for learning how to implement and operate Cisco enterprise network core technologies. By focusing on real-world skills, each chapter prepares you with the knowledge you need to excel in your current role and beyond. It covers emerging and industry-specific topics, such as SD-WAN, network design, wireless, and automation. This practical guide also includes lessons on: ? Automation ? Network assurance ? Security ? Enterprise infrastructure ? Dual-stack architecture ? Virtualization In addition to helping you gain enterprise knowledge, this study guidecan lead you toward your Cisco specialist certification. When you purchase this guide, you get access to the information you need to prepare yourself for advances in technology and new applications, as well as online study tools such as: ? Bonus practice exams ? Pre-made flashcards ? Glossary of key terms ? Specific focus areas Expand your skillset and take your career to the next level with CCNP Enterprise Certification Study Guide.

This book constitutes the refereed proceedings of the 24th Nordic Conference on Secure IT Systems, NordSec 2019, held in Aalborg, Denmark, in November 2019. The 17 full papers presented in this volume were carefully reviewed and selected from 32 submissions. They are organized in topical sections named: privacy; network security; platform security and malware; and system and software security.

Software Defined Networking (SDN) stellt einen ziemlichen Paradigmenwechsel im Netzwerkumfeld da. Heutige Netzwerke werden nach wie vor relativ statisch konfiguriert. Es gibt dynamische Routingprotokolle die dafür geschaffen wurden, Ausfälle zu erkennen und den Verkehr dann über andere Wege zu leiten. Den richtigen Lösungsweg zu finden, stellt sich aber teilweilse sehr komplex dar. Außerdem werden die Geräte (Router, Switche, Firewalls) in der Regel einzeln konfiguriert. Einen neuen Datenpfad zu schaffen, erfordert daher von den Administratoren viele einzelne Arbeitsschritte, ein Fehler in einem dieser Schritte (z.B. ein Tippfehler in einer IP-Adresse) und der ganze Pfad funktioniert nicht. Netzwerkgeräte haben in der Regel eine sogenannte Control Plane, welche die Steuerung übernimmt (welche Daten sollen wo lang fließen) und die Data Plane in welcher (häufig mit Hardwarebeschleunigung) aufgrund der Regeln der Control Plane die eigentlichen Daten fließen. Jedes Netzwerkgerät besitzt in der Regel eine eigene Control Plane und muss deswegen einzeln konfiguriert werden. Die Idee hinter SDN ist nun, die Control Plane zu zentralisieren. Erst Konzepte stammen so etwa aus dem Jahr 2005 aus den USA. Ein zentraler Controller kann wesentlich „intelligentere“ Entscheidungen treffen, da er den Zustand des Gesamtnetzwerkes kennt. Über ein Steuerprotokoll kann er dann den Geräten Anweisungen geben, welche Pakete über welchen Pfad weiterzuleiten sind. Damit sind wesentlich komplexere Entscheidungen möglich und auch das schnelle Umleiten von Verkehr ist möglich. Das momentan marktführende Protokoll heißt OpenFlow und und wird von der Open Networking Foundation weiterentwickelt. Das wirklich interessante dabei ist, das in den neueren OpenFlow Versionen die Trennung der ISO-Schichten 2 – 4 eigentlich aufgeweicht wird und auch dies dazu beiträgt, dass durch komplexere Entscheidungen möglich sind. Die Controller erlauben es, eigene Programme über ein Programmier-Interface einzuklinken und damit kann sich der Netzwerkadministrator vom statischen Netzwerk der Vergangenheit verabschieden und das Netzwerk wirklich programmieren. Das Buch soll nach einer Einführung in die Theorie, die sich aber auf ein Kapitel SDN allgemein (viele Hersteller verkaufen unter SDN nur eine leicht flexiblere Konfigurierbarkeit Ihrer Komponenten) und einem Kapitel, welches den OpenFlow Standard erklärt (in seinen verschiedenen Versionen) dem Leser das Thema praktisch näherbringen. Dazu wird gezeigt, wie nur durch das „einschieben“ von Flows Regeln auf OpenFlow fähige Geräte gebracht werden können. Ein Kapitel wird sich mit den Möglichkeiten bzw. Limitierungen tatsächlich OpenFlow fähiger Geräte beschäftigen. Und schließlich führen wir in die APIs der beiden Controller Floodlight und OpenDayLight ein, damit der Leser danach seine eigenen Ideen mit diesen APIs umsetzen kann, um das eigene Netzwerk zu Programmieren.

This book constitutes the refereed post-conference proceedings of the 14th EAI International Conference on Quality, Reliability, Security and Robustness in Heterogeneous Networks, QShine 2018, held in Ho Chi Minh City, Vietnam, in December 2018. The 13 revised full papers were carefully reviewed and selected from 28 submissions. The papers are organized thematically in tracks, starting with security and privacy, telecommunication systems and networks, networks and applications.

This book constitutes the thoroughly refereed post-workshop proceedings of the 22nd International Workshop on Security

Protocols, held in Cambridge, UK, in March 2014. After an introduction the volume presents 18 revised papers each followed by a revised transcript of the presentation and ensuing discussion at the event. The theme of this year's workshop is "Collaborating with the Enemy".

Software Defined Networking is revolutionizing the networking world. While the industry transitions to a software-centric architecture, a clear definition of SDN remains murky at best. This book clarifies the current industry confusion about what SDN is, why it's important, and most importantly the protocols and use cases that define SDN. OpenFlow (OF) is a critical piece of the SDN puzzle. While SDN solutions exist that do not require OF, it is undeniable that OF helped spur the innovation in SDN. The history of OF, its current and future status, and the associated use cases will be explained in detail in this book. Lastly, the book attempts to lay out SDN deployments that are real and current today, and apply practicality to the vast world of SDN architectures.