Journal of Computer Networks, Architecture and High Performance Computing
Volume 3, Number 1, January 2021
https://doi.org/10.47709/cnahpc.v3i1.998

Submitted : 2021-06-24
Accepted : 2021-06-27
Published : 2021-06-29

Design of captive portal LAN with redundancy connections

Arie Budiansyah[1)*], Dirja Nur Ilham[2)], Rudi Arif Candra[3)]
[1]Universitas Syiah Kuala, Indonesia [2)3)]Politeknik Aceh Selatan, Indonesia
[1)]arie.b@unsyiah.ac.id, [2)]dirja@poltas.ac.id, [3)] rudiarifcandra@gmail.com

ABSTRACT

A captive portal network is a computer network that uses a web page as an authentication to enter the network. The back end of the authentication process can use Radius, Kerberos, or LDAP with the AAA mechanism. This captive portal mechanism is starting to be in great demand for use in schools, offices, campuses, housing because each user has a separate account that does not share such as the WPA PSK authentication security method. However, if the captive portal is implemented with a redundant connection through the application of a ring topology, it will experience network loops. This is because 2 ethernet ports of the captive portal framework are connected via a ring topology. The captive portal authentication process managed at the application layer or layer 7, while the principle of the communication mechanism between devices in the network uses the IEEE 802 standard or ethernet. This standard specifies the physical functions of IEEE 802.3 and IEEE 802.2 data link layer as the main part of the LAN ethernet protocol. From this we see that the captive portal network with redundancy is a tiered mechanism. The results of this research describe 2 examples of captive portal network designs with redundant connections to frameworks that can be used. Naturally the network traffic flow is like the letter U but if one of the intermediary devices disconnected or power off then the device below it will use an alternate path or ether3 framework port like number 11. Some of the traffic flow will go to the ether2 port and some go to the ether3 port of the captive portal framewok and the disconnected intermediary devices don't interfere with the device below.

Keywords: captive portal; authentication; loops; redundancy connection; spanning tree protocol; alternate path; media converter twisted pair to fiber optic

INTRODUCTION

In general, the network topology is divided into 2 types, namely physical topology and logical topology (McMillan 2015)(Behrouz A. Forouzan 2012)(Andrew S. Tanenbaum 2012). What is meant by physical topology is that it illustrates the physical location of intermediary devices and end devices, while what is meant by logical topology is that end devices are connected to which intermediary devices, what media transmission is being used. There are also those who describe network topologies in the form of classifications such as star topology, tree, ring, mesh, hybrid, multi drop, fully connected and multiply connected (McMillan 2015)(William J. Barksdale 1982). In short, these two views on topology are always used in the presentation of network analysis and design so that the user's needs for the network are clearly described and the user understands the system requirements that must be met (James D. McCabe 2007). Currently network technology uses the IEEE 802 standard or known as ethernet as a communication standard between network devices from various manufacturers. This standard specifies the physical functions of IEEE 802.3 and IEEE 802.2 data link layer as the main part of the LAN ethernet protocol as shown in Figure 1 (Behrouz A. Forouzan 2012). In detail, IEEE 802 describes the data link layer in 2 sub layers, namely Logical Link Layer (LLC) and Media Access Control (MAC) and several sub layers in the physical layer such as Ethernet physical layer, token ring, token bus and so on. The thing that is easily recognizable from this ethernet technology is the existence of a box called a switch (SW) as an intermediary or intermediary between end devices. SW devices are intermediary devices that connect point-to-point intermediary devices and end devices through the ports on the SW (Andrew S. Tanenbaum 2012).

* Corresponding author

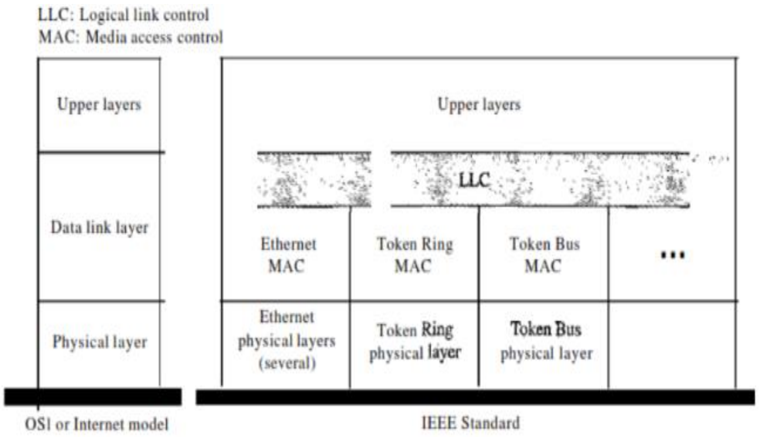

Fig.1 The Physical and Data Link layer as main part ethernet protocol. (Behrouz A. Forouzan 2012)

The main goal in designing a network is not only connecting intermediary devices and end devices, but reliable networks must also be considered (Cisco Networking Academy 2020). There are at least 4 reliability factors in the network, namely fault tolerance, scalability, Quality of Services (QoS) and network security. What is meant by fault tolerance factor is the existence of multipaths as the main path and alternate path. The scalability factor is that the network can be expanded or enlarged quickly and easily to support users and applications without affecting the performance of existing services. QoS is a mechanism to ensure reliable delivery of content for all users, for example content delivery within the ITU or IETSI latency and packet loss time range (Budiansyah and Iqbal 2019)(Hasanul Fahmi 2018). Network security is a mechanism for securing network physical infrastructure and information security. In this research fault tolerance factor will be added to the captive portal network due to user requests. The fault tolerances function will maintain a redundant connection in traffic going to the main captive portal frameworks. If the main path of the captive portal framework is broken, fault tolerance will automatically move connections to an alternate path to the main captive portal framework. Fault tolerance mechanism is very important in maintaining a reliable captive portal network framework (Cisco Networking Academy 2020).

However, before fault tolerance was applied to the network, an initial problem was found, authentication to the network. A captive portal network is actually a network that implements protocols such as radius or kerberos, LDAP with the Authentication, Authorization, and Accounting framework, abbreviated as AAA as a security mechanism for entering the network (Xia and Brustoloni 2004)(Jonathan Hassell 2002). The captive portal itself is a web page for the user authentication portal to enter a username and password and its managed on application level or layer 7. Only users and devices that have accounts or have authentication can log on to the LAN network. From this we see that the captive portal network with redundancy is a tiered mechanism, namely the first authentication process and the last fault tolerance process.

LITERATURE REVIEW

The main problem with fault tolerance is the emergence of network loops on redundant connections to the SW itself as shown in Figure 2. Redundant connections are basically a bridge logic topology where one connection line must be disabled and only one path is active (Andrew S. Tanenbaum 2012; Behrouz A. Forouzan 2012; Rich Seifert 2008). Theoretically a bridge is a SW device in which several Ethernet ports are logically combined (bridged) for full duplex communication between devices. Bridge port mode means that there is no difference using ether2, ether3, ether4 and so on ports on the SW because these ports will be considered an ethernet port. This bridge port system is automatically found in the unmanageable SW type, but in the manageable SW a bridge configuration is required for the unification of logical bridge ports. There is already a solution to this problem, namely the Spanning Tree Protocol (STP) or Common Spanning Tree (CST) service found in the SW. Many researches on STP have also been carried out and fault tolerance mechanisms are no longer a problem and are easy to implement to make the network more reliable.

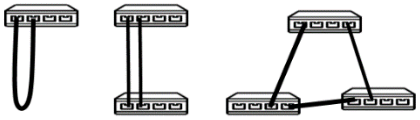

Fig.2 The three types of loops in network topologies.

However, STP works at layer 2 with 802.1x architecture while the captive portal network works at the application level layer 7 to authenticate devices and users before being able to connect to the network (Internet Engineering Task Force (IETF) 2020)(Marques, Zúquete, and Barraca 2019). If a devices has successful authenticated then communication in LAN works at layer 2 maintained by each SW. In these days, a varian STP has been developed such as STP, RSTP (Rapid Spanning Tree), MSTP (Multiple Spanning Tree), PVST+ (Per VLAN Spanning Tree), Rapid PVST+ (Rapid Per VLAN Spanning Tree) (Cisco Networking Academy 2020; Rich Seifert 2008). These varians of STP has own characteristic but can be categories in 2 purposes. One for convetional redundant link in bridge network, STP and RSTP. One for VLAN redundant link in bridge network, PVST+ and Rapid PVST+. All of those STP worked in bridge network to maintain fault tolerances.

However, at this stage there is a challenge how to integrate captive portal services and redundant connections services. The captive portal mechanism implements authentication through the web page or application layer and not through the layer 2 layer. The issue of security of sensitive information transactions is a concern for the captive portal network, especially in the authentication process via wireless. In this study, there is no problem with wireless captive portal authentication, but the problem lies in authentication via wired intermediary devices such as SW and Wi-Fi access points to the captive portal framework. Prior to the authentication process at the application layer, devices cannot connect to each other. However the binding mechanism can bypass the authentication process to web pages and the device can connect to the captive portal network. Once connected, the fault tolerance mechanism can be designed to be placed as a redundant connection framework captive portal. This study will describe several forms of captive portal network designs with redundancy connections that can be implemented in schools, offices, campuses easily and quickly.

In the process of full duplex data communication between devices, the SW bridge device uses a filter called the Static Address Table (SAT) which stores the MAC Address and port number of the device connected to its port. The SW bridge device checks the destination MAC address of a frame and decides whether to forward or drop the frame. In simple terms, the SW bridge function includes 2 things, namely learning and forwarding frames. If a station 0 (S1) sends Frame0 (F0) to destination S2 and reaches Bridge1 (B1) via Port 0 (P0). B1 will record S1's MAC Address and S1's port number and broadcast a copy of F0 to all ports except P0. Since there are 2 paths from B1 to B2, there will be 2 frames (F1 and F2) sent from B1 to B2. Because B1 receives 2 frames and B2 also broadcasts to all ports except ports F1 and F2. B2 receives a response from S2 on port 4 (P4) and B2 responds by giving F3 and F4 containing the MAC Address of S2 to B1. Here B1 will record S2's MAC Address on P3 and P4 and this is not allowed by the SAT filter and B1 drop frame and repeat sending F1 and F2 and so on. The figure 4 descibed a loops generate by B2 and B1 from full duplex communication S1 to S2 stations.

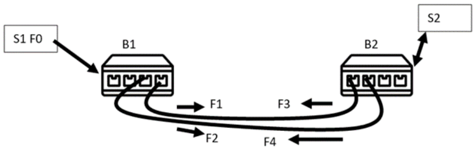

Fig. 3 F3 and F4 are loops as impact of F1 and F2 frame.

To be able to automate path switching like this, initially between SW devices will exchange BPDUs to determine the Root Port (RP), Designate Port (DP) or Alternate Port (AP). The situation of network loops is overcome by activating a spanning tree protocol such as the Spanning Tree Protocol (STP 802.1D), Rapid Spanning Tree Protocol (RSTP 802.1W) or Multiple Spanning Tree Protocol (MSTP 802.1S). LAN traffic flow will move from DP to RP and vice versa in full duplex communication and the AP port becomes an alternate path if the main path is down.

METHOD

As discussed earlier, in designing a network, it is not just connecting end devices and intermediary devices, but the reliability of networks needs to be considered. The first step in designing a network is how to produce a design that is logical (logical), can be an example or reference (reproducible) and has the ability to last a long time and is good (defensible) (James D. McCabe 2007) According to James D. McCabe in his book entitled *Network Analysis, Architecture, and Design*, there are at least 3 steps in designing a network, The first, analyzing the network, secondly, conceptualizing the network architecture and finally designing the physical and logical network.

First step and also the main key in analyzing requirement of network are gathering the users and application requirements and then match it with the appropriate network system. We must be able to find match network systems that are in accordance with user and application requirements. After stackholder agreed about network system, the next step is to make a picture of conceptual image of the network architecture. The function of this conceptual network is an initial prototype for the next step which is the network design of physical and logical topology. The stages of this method of McCabe can be seen in table 1. In the case of this study, first, the user requirement is a captive portal network with redundancy connections and a network system that can fulfill captive portal services is a MikroTik router which includes captive portal services. As for routers such as Cisco, Juniper, OpenWRT but must use a PC Server as a captive portal with Remote Authentication Dial-In User Service (Radius) software (Internet Engineering Task Force (IETF) 2019). At this stage the decision must be made to use the router system with what brand? Second, request redundancy connection to the captive portal framework.

Table 1 Details of three steps for network designs

No	**Step for Network Design**	**What you do?**	**1st Note**	
1st	Network Analysis	User requirements	Captive portal LAN with redundancy to framework.	
				2nd Note
		System requirements	SW included captive portal services?: A	**A**
			SW excluded captive portal?: B	
			Where location of redundancy connection will implemented?	To the framework captive portal.
2nd	Network Architecture	Draw the conceptual of network diagram	Figure 2.	
3rd	Network Design	Draw Physical and logical topology	Figure 3	

To solve this integration problem, a more in-depth analysis is needed. The network analysis process diagram is divided into 2 parts, namely requirements analysis and flow analysis. The function of requirements analysis is the process of determining the fundamental requirements that the network needs to be able to properly support users, applications and network devices. The function of flow analysis is to analyze the user, application, device, and network requirements based on their end-to-end characteristics. Flows (also known as traffic flows or data flows) are sets of network traffic (application, protocol, and control information) that have common attributes, such as source/destination address, type of information, directionality, or other end-to-end information. In the figure 4 at left part, traffic flow of ethernet LAN like letter ‘U’ from the last end devices to the main router captive portal. On the right part, we found a sink in main router if we directly connect a cable in to. By analyzing the flow, it will be known the direction of traffic movement during the authentication process on the captive portal service as shown in Figure 3.

Without redundancy networks the direction of traffic movement is also the same. When installing redundancy networks, the direction of traffic movement changes, partly towards the left and partly towards the right. By analyzing the requirements as shown in Figure 4, the fundamental requirements of the network will be known which have gone through several stages such as gathering and list requirements, developing services metrics and characteristic behavior which are the result of developing requirements and Map requirements.

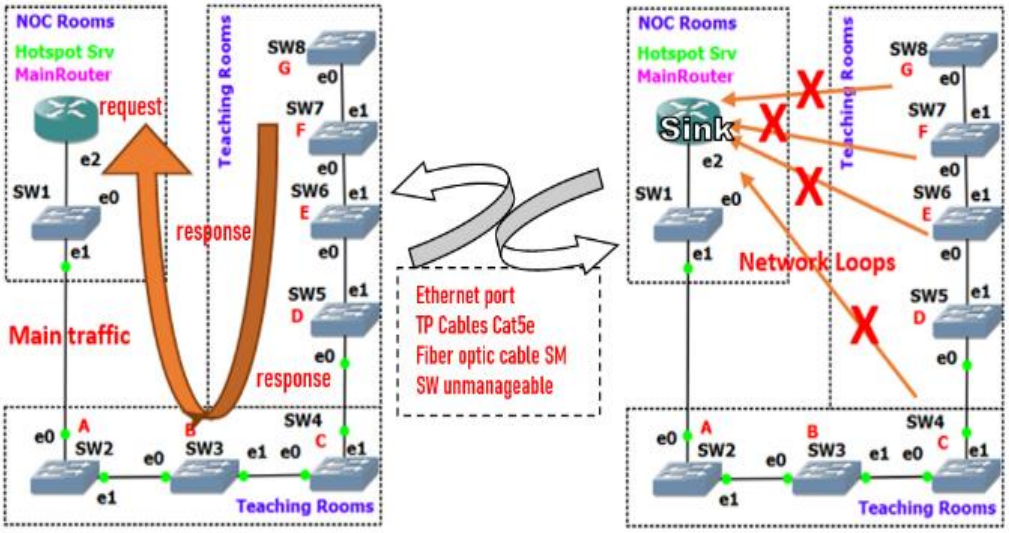

Fig.3 Traffic flow of LAN and posiblity of loops on main router captive portal.

From the conceptual results of the network in Figure 4, The two type design of captive portal LAN are made with redundant connections to the captive portal framework. The first design is using a TP cable and the second design using a Fiber Optic (FO) cable with Media Converter TP to FO media transmission. Both network designs use a ring topology and in bridge network but can be developed with a tree, star or chain topology as long as the topology pattern followed in the first or second design drawings topology. Table 2 records flow analysis as knowledge material in creating redundant connections in the captive portal framework.

Table 2 Logic table of Captive portal networks with redundancy.

No	System Requirement for Captive Portal Redundancy	Flow Analysis
1.	Two pieces of intermediary devices SW. 1st SW for framework captive portal. 2nd SW for alternate path to framework.	Before redundancy: All devices will do a req authentication process to main router via ether2 framework captive portal.
	Brand intermediary device: MikroTik	
	Topologi: Ring	
	Mode Port: Bridge Type Port: RSTP	
	Services: 1st SW: Hotspot, Bridge, RSTP 2nd SW: Bridge, RSTP	
	Port connections each SW:	After redundancy: All devices will do a req authentication process to main router via ether2 too but if some link broken half devices via
	1st SW: - ether1 to WAN - ether2 to ether0 SW (main path)	

- ether3 to ether0 2nd SW (Alternate path) 2nd SW: - ether0 to ether3 1st SW	ether2 1st SW and half devices via ether0 2nd SW to ether3 1st SW.
Cables: Twisted Pair or Fiber Optic SM with MC	

RESULT

In the first captive portal design as described in figure 5, the cable used TP cables connected from ether2 1st SW to ether0 SW1, this is the main path of traffic flow. Next, ether3 to ether0 2nd SW RSTP, this is the alternate path. The ether0 will be used as WAN. However each ethernet port of the connected device will act as RP and DP starting from the first SW to the last and the AP port will forever be disabled if the main backbone line is still alive. However, if the main line is cut off at any point, the DP will automatically be active as a new device line. Under normal circumstances the traffic direction is like forming the letter U and when one point is cut off, the traffic direction is like number 11 with the appearance of 2 lanes. A line goes to the left ether port and a line moves to the right ether port.

The second port captive design is very interesting because it uses FO transmission media as described in figure 6. The use of media converter (MO) FO to UTP eliminates the RP, DP and AP functions of each SW port. The ring topology is still used in the second design but the backbone device is no longer SW but MC. From the operational side, the power supply using MC is only 5 Vdc more efficient than SW requires 12 - 48 Vdc. In the daisy chain topology, the PSU MC mechanism can be independent using solar panels or a small dc permanent magnet generator. In rural areas where electricity supply is still difficult, the use of the second captive portal design is better than the use of the first design. Even though at some points the electricity supply is cut off, if the PSU MC comes from a solar panel, it has no effect at all and the network continues to run until the last point or the traffic direction continues to form the letter U. Unless one of the MCs dies, the traffic direction forms the number 11.

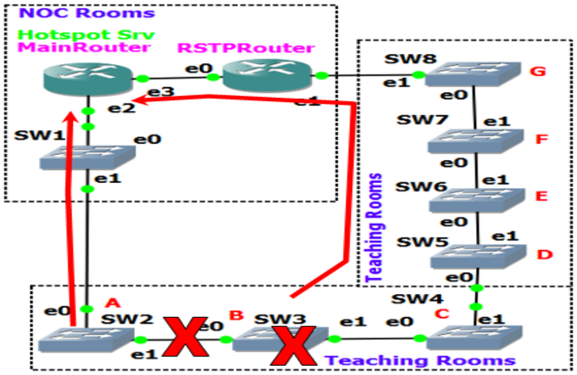

Fig.5 The 1st design of LAN captive portal with redundancy using TP cables.

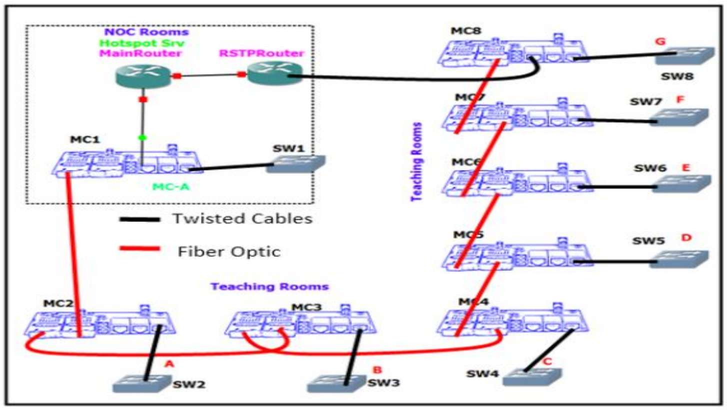

Fig.4 The 2nd design of LAN captive portal with redundancy using MC FO to TP cables.

Journal of Computer Networks, Architecture and High Performance Computing
Volume 3, Number 1, January 2021
https://doi.org/10.47709/cnahpc.v3i1.998

Submitted : 2021-06-24
Accepted : 2021-06-27
Published : 2021-06-29

DISCUSSIONS

In general, the design of a LAN where the distance between intermediary devices is far enough around 20 meter to 100 meter and the redundancy services required by user, this condition only possible if implementation for redundancy connection at central of framework. If the distance more than 100 meter, we could use media converter FO to TP. Although, we use FO cable transmission but this is not part of Fiber Optic To The Home (FTTH) technology. The media converter helped to extend as far as it cound up to 5 kilometer and it has a right posibility to implement in the rural area such as small village.

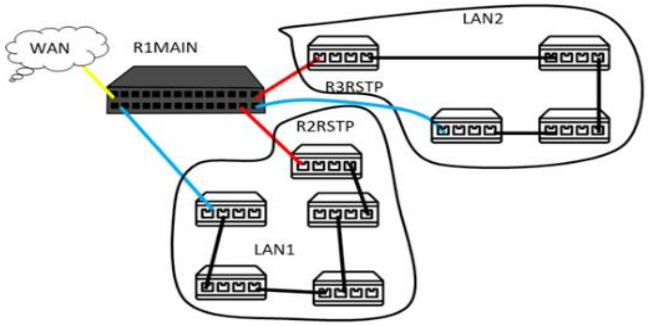

Fig.6 The conceptual topology of captive portal LAN with redundancy connection to main path R1MAIN.

We considered the backbone transmission is expected to stay alive in order to maintain the direction of traffic movement like the letter U in figure 4. The STP protocol used is RSTP although in practice other methods can be used. The choice of RSTP is only as evidence that the captive portal service and the STP protocol can run integrated with each other even though the two are not at the same layer. To be able to do this integration, the captive port framework and the RSTP router must be separated and not in 1 captive portal router, although in some studies the loops pattern can only use 1 SW as shown in Figure 1. The loop pattern with the captive portal design is required to use a loop pattern of at least 2 SW while still separating the captive portal framework.

REFERENCES

Andrew S. Tanenbaum, David J. Wetherall. 2012. *Computer Networks 5th Ed.* 5th Ed. Pearson.

Behrouz A. Forouzan. 2012. *Data Communications and Networking: Forouzan, Behrouz A.: 8601400052488: Amazon.Com: Books*. 5th Ed. McGraw-Hill Education.

Budiansyah, Arie, and M. Iqbal. 2019. “A Testing Packet Delay Variation and Packet Loss Problem on Local Area Network Based on ITU-T Standard.” in *IOP Conference Series: Materials Science and Engineering*. Vol. 506. Institute of Physics Publishing.

Cisco Networking Academy. 2020. *Introduction to Networks Companion Guide (CCNAv7): 9780136633662: Computer Science Books @ Amazon.Com*. Cisco Press.

Hasanul Fahmi. 2018. “Analisa Pengukuran Delay, Jitter, Packet Lost Dan Throughput Untuk Mendapatkan Kualitas Peforma Radio Streaming Yang Baik Pada Radio Simfoni Fm Malang.” *Jurnal Teknologi Informasi Dan Komunikasi* 7(2):98–105.

Internet Engineering Task Force (IETF). 2019. “Dynamic Authorization Proxying in the Remote Authentication Dial-In User Service (RADIUS) Protocol Rfc 8559.” *Ietf.Org*. Retrieved June 21, 2021 (https://datatracker.ietf.org/doc/html/rfc8559).

Internet Engineering Task Force (IETF). 2020. “Captive Portal Architecture Rfc 8952.” Retrieved June 20, 2021 (https://datatracker.ietf.org/doc/html/rfc8952).

James D. McCabe. 2007. *Network Analysis, Architecture, and Design: A Volume in The Morgan Kaufmann Series in Networking*. 3rd Ed. Morgan Kaufmann.

Jonathan Hassell. 2002. *RADIUS [Book]*. O’Reilly Media, Inc.

Marques, Nuno, André Zúquete, and João Paulo Barraca. 2019. “Integration of the Captive Portal Paradigm with the

Submitted : 2021-06-24
Accepted : 2021-06-27
Published : 2021-06-29

802.1X Architecture.” *Arxiv.Org*.

McMillan, Troy. 2015. *Cisco Networking Essentials: McMillan, Troy: 9781119092155: Amazon.Com: Books*. Vol. II. 2nd edition. Sybex.

Rich Seifert, James Edwards. 2008. *The All-New Switch Book: The Complete Guide to LAN Switching Technology, 2nd Edition | Wiley*. 2nd Ed. Wiley.

William J. Barksdale. 1982. “Practical Computer Data Communications: Overview of Data Communications.” Pp. 7–22 in. South TEC AssociatesHuntsvilleUSA: Electronic Conventions Inc.

Xia, Haidong, and José Brustoloni. 2004. “Detecting and Blocking Unauthorized Access in Wi-Fi Networks.” *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 3042:795–806.