Journal of KONBiN 39 (2016)
ISSN 1895-8281
DOI 10.1515/jok-2016-0031 ESSN 2083-4608

BRING YOUR OWN DEVICE - PROVIDING RELIABLE MODEL OF DATA ACCESS

BRING YOUR OWN DEVICE - NIEZAWODNY MODEL DOSTĘPU DO DANYCH

Paweł Stąpór, Dariusz Laskowski

Wojskowa Akademia Techniczna im. J. Dąbrowskiego

e-mail: dariusz.laskowski@wat.edu.pl

***Abstract**: The article presents a model of Bring Your Own Device (BYOD) as a model network, which provides the user reliable access to network resources. BYOD is a model dynamically developing, which can be applied in many areas. Research network has been launched in order to carry out the test, in which as a service of BYOD model Work Folders service was used. This service allows the user to synchronize files between the device and the server. An access to the network is completed through the wireless communication by the 802.11n standard. Obtained results are shown and analyzed in this article.*

***Keywords:** availability, reliability, BYOD, data transfer*

***Streszczenie:** W artykule przedstawiono model Bring Your Own Device (BYOD), jako model sieci teleinformatycznej, która oferuje użytkownikowi niezawodny dostęp do zasobów sieciowych. BYOD jest modelem dynamicznie rozwijającym się, znajdującym zastosowanie w wielu dziedzinach.. W celu przeprowadzenia badań została uruchomiona sieć badawcza, w której jako usługę modelu BYOD zastosowano usługę Work Folders. Usługa ta umożliwia użytkownikowi synchronizację plików pomiędzy urządzeniem a serwerem. Dostęp do sieci został realizowany poprzez łączność bezprzewodową wg standardu 802.11n. Otrzymane wyniki badań zostały przedstawione i przeanalizowane w poniższym artykule.*

***Słowa kluczowe:** dostępność, niezawodność, BYOD, transmisja danych*

BRING YOUR OWN DEVICE - PROVIDING RELIABLE MODEL OF DATA ACCESS

1. Introduction

Recent years are a time of rapid development of technology and innovation. It is also the time in which newer technologies are more affordable for people and equipment used by them have more and more advanced and sophisticated features. Now, in the age of smartphones and tablets, and universal access to the Internet, the mobile phone has taken over the majority of computer functions, and also has some that facilitate various tasks. According to the report Polska.Jest.Mobi 2015 prepared in cooperation with TNS Poland in May 2015 almost 19 million smartphones are used by Poles aged 15+ that is 58% of the Polish population. Users use their mobile devices i.e. laptops, tablets or smartphone for different tasks. There was even an idea that employees can use their private devices in the workplace, to perform their tasks. This new concept was created, as it was noted that employees have devices that are more modern and more efficient than those offered to them by the employer. Therefore was created model concept Bring Your Own Device (BYOD).[1,2] It rapidly developed solution is implemented in different areas by different suppliers providing services in the area of ICT [10,11,12]. This publication is aimed to check the reliability of the implementation BYOD model, providing the user an access to data at the required level of quality.

2. Characteristic of BYOD model

Bring Your Own Device is a model that allows the user tasks regardless the place of dislocation and conditions of the network, using private devices.[3] BYOD model should offer the user to wireless (mobile) and wired access. This access should be implemented using the latest standards. The wireless implementation of user service can be divided into two ways.[4] The first is an access via the wireless LAN, using standard 802.11n and 802.11ac/d by access point e.g. in the workplace. The second way is to access via a mobile network (e.g. 3G/4G, WiMAX, WiMAX-2, LTE, LTE-A, etc.). The wired access can be implemented using standard Fast Ethernet or Gigabit Ethernet. The only disadvantage of this model is incorrectly protected mobile devices and the possibility of non-compliance by employees of security policy, but this may occur to any network solution.[5,6]
As mentioned the BYOD model is widely used and can be implemented in many different ways depending on demand. Due to the complexity of the model BYOD is recommended that an analysis of the individual segments of the whole model. The general model shown below (Fig. 1) can be divided into three segments. The first one concerns the place where data is stored or applications that users can remotely use. The second segment is an area of implementation of the routing and service access.

This area includes network infrastructure e.g. company, architecture internet service provider (ISP) and network access infrastructure - wired or mobile. The third segment is the user's device - a device specification, security methods, characteristics of network application, etc. Each segment may be analyzed in various aspects – safety [13], performance, reliability or QoS [7,8,9]. In this article all segments were analyzed and the analysis according to reliability was checked.

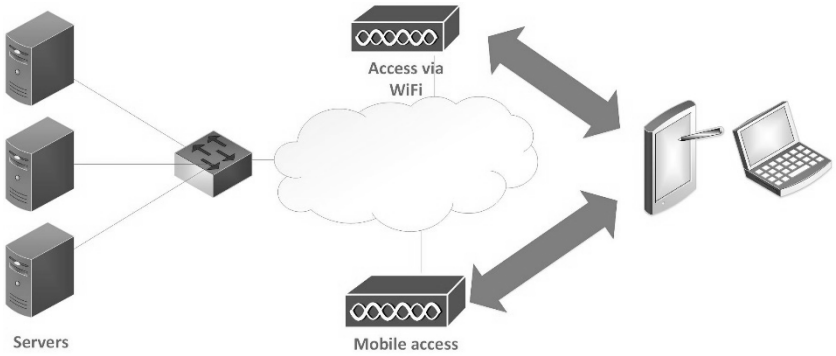


Fig. 1. General architecture of Bring Your Own Device model

3. Research model

The research model is presented below (Fig. 2). To configure tested IT network widely used network devices were used, some more important are as follows: routers, the Cisco 28xx and 29xx, 24 port switches 3COM family Baseline 22xx, wireless routers Cisco Small Business WRVS4400N and two servers Hewlett-Packard family Proliant DL 360 generation 5 with Windows Server 2012 R2 configured with services including Active Directory, DNS and Work Folders, etc.

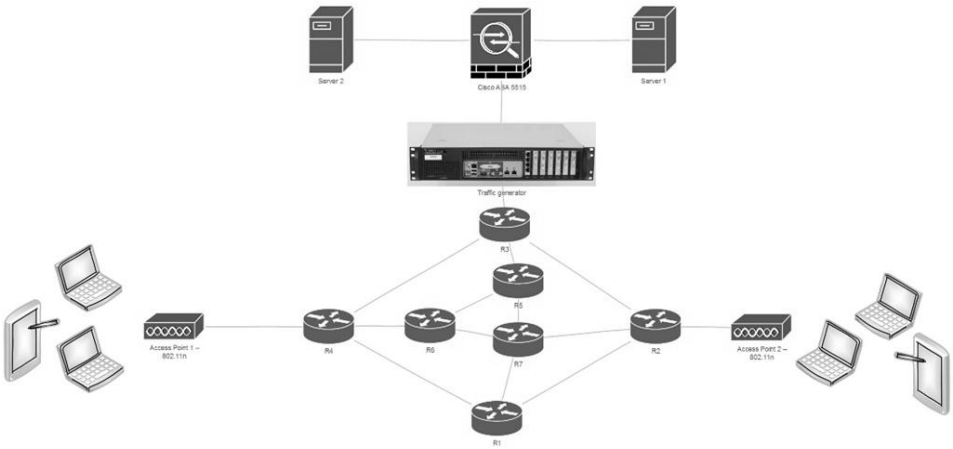


Fig. 2. Architecture of research model

The confidentiality of communication is achieved through VPN tunnels using protocol SSLv3.0. This architecture provides the user with a wired and mobile access. On the client's device Windows 10 has been installed and wired communication network is available via the network interface Gigabit Ethernet, and wireless interface using 802.11n. Routing using OSPF was used in the network and the devices were addressed with the use of IPv4 addresses. Work Folders were used as a network service.

The service allows working folders to synchronize files between the server and the users. The principle of operation is similar to applications such as OneDrive or Dropbox. The difference is that in the case of the service data is stored on the local server rather than on a server owned by others for authentication is required account and domain password. Work Folders uses HTTPS and SSL certificate to ensure the confidentiality of data. The server administrator can delete the files in the working directory user and secure them in such a way as to minimize the risk of unauthorized use of files in a way [1]. The test model also placed a device that emulates network traffic - LANforge ICE CT50. In addition, this study involved few additional mobile devices, so as to provide additional load on the access points. On this BYOD model was carried out the following tests:

- Examined the probability of failure services, depending on the number of services running on the network. The number of services increases from 1 to 100. For each instance a 80 iterations to obtain the most reliable results. As the time limit for realization of services taking 60 seconds. Research carried out for three wireless standards: 802.11g, 802.11n and 802.11ac.
- Examined bandwidth and delay variation network user who has access to the network using 802.11n. Incorporating the results of the previous study, it was assumed that the test will be performed for the network, which is running 10 services. Moreover, the network for packet loss as a function of time was examined.

4. Results of research and analysis

The results prepared graphs the probability of failure services, depending on the number of running services have been prepared on the basis of the study (Fig. 3). The probability of failure services was calculated as the ratio of unrealized services to the number of requisition for the service, i.e. 80 repetitions. For this probability subjectively acceptable level and critical was determined. It increased to 0.15 - acceptable level, 0.25 - critical level.

As can be seen from the graph (Fig. 3), the best results were obtained for 802.11ac standard. Probability started to grow only at 35 services running on the network at the same time, while the 802.11g standard was 8 services. This gives more than four times the reliability of the network.

It also means that by using the latest standard WiFi network at the same time can be used by four more times users. It can be concluded that by introducing newer standards, and thus higher bandwidth networks, greater reliability of the network and access to network resources can be provided. It is also worth noting that the probability of these three standards did not reach the level above 0.8 (802.11g). This means that there is always a probability that our demand for service will be completed even at a very busy network.

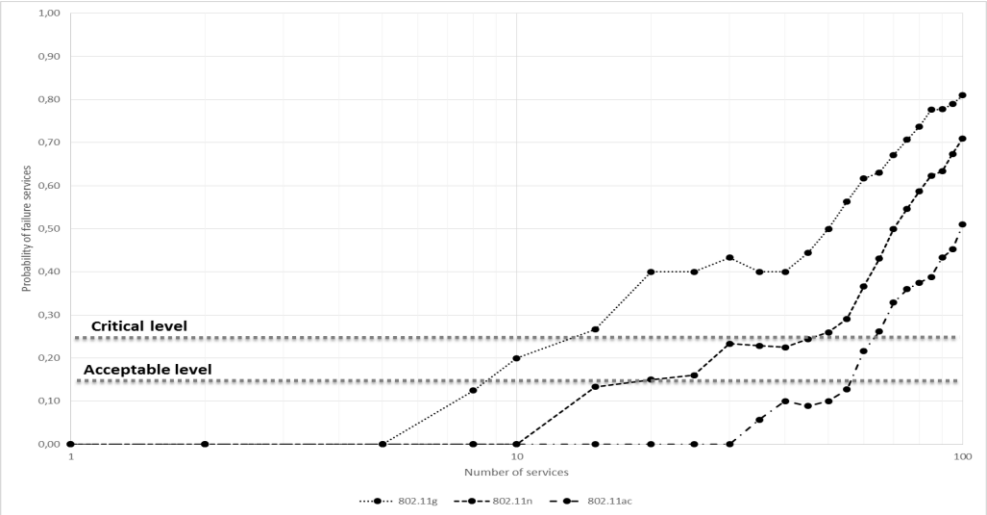


Fig. 3 The probability of failure to the service depending on the number of services

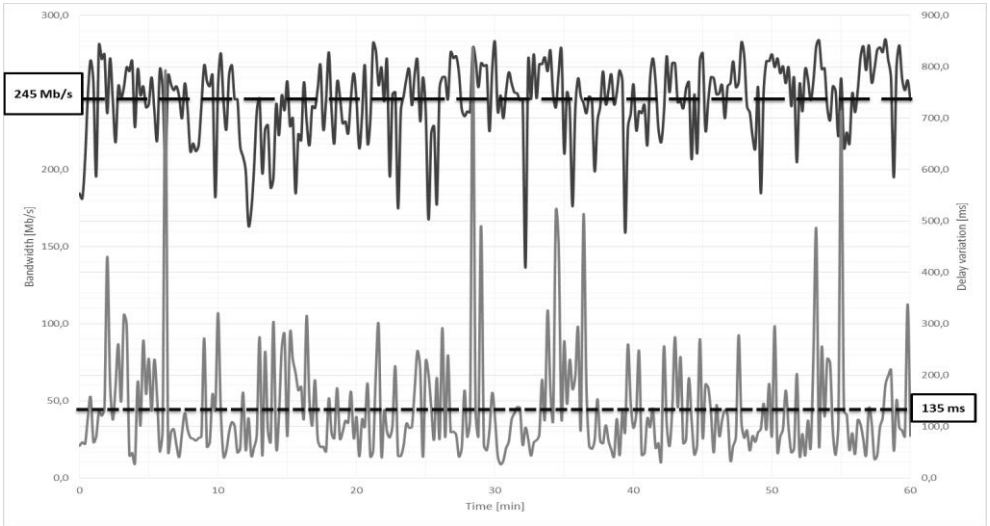


Fig. 4. Bandwidth and network delay variation as a function of time for 802.11n standard

Then the network in terms of bandwidth and delay variation was tested. On the basis of the results the graph below was drawn (Fig. 4).
An average throughput for 802.11n standard increased to 245 Mb / s. It seems to be quite a good result, especially since at the same time the system was used by 10 users. Jitter at an average level of 135 ms is a value acceptable for the network. The maximum value in the range of 300 - 850 ms, are temporary and do not actually visible to the user. In this network delay variation has no significant impact on the quality of service, because the network is not used to transmit packets in real time, i.e. it is not supported Internet telephony VoIP or streaming video.

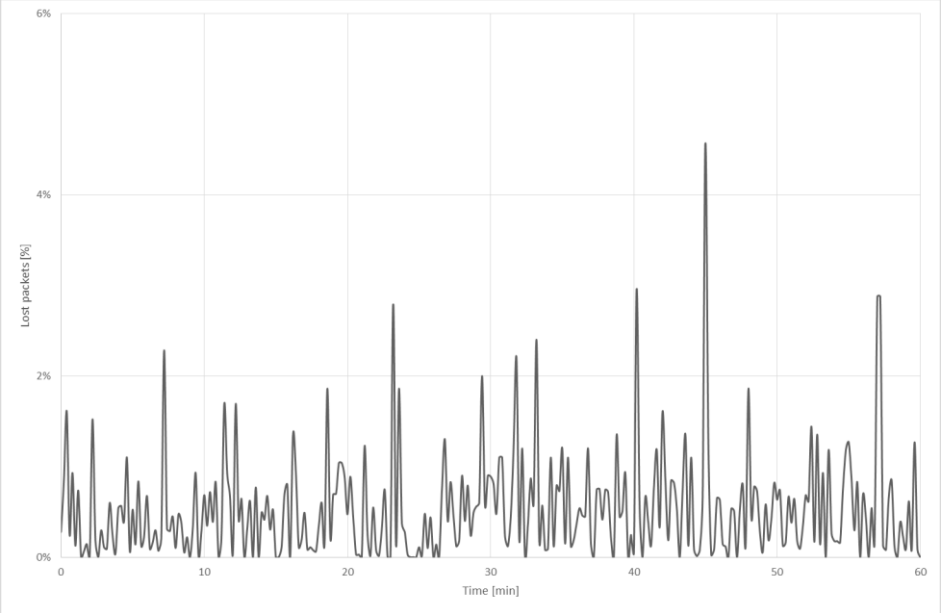


Fig. 5. Packet loss in the network as a function of time

The last study was aimed to investigate the network using BYOD model in order to check a packet loss. The results are presented in the graph (Fig. 5). The observation time was 60 minutes, to more accurately portray the situation in the network, and thus get more objective results. As can be seen, the average packet loss does not exceed 1%, which is a very satisfactory result. Momentary higher packet loss was due to more traffic in the network. It did not affect the use of services, thus providing reliable service significantly.

5. Conclusions

The article examined by BYOD model reliable access to network resources using a mobile standard. The test results show that, depending on the standard used a wireless network is able to handle user with the probability depending on the number of simultaneously running network services.

The user using the services of BYOD model has provided reliable access to network resources with bandwidth and latency variability at a satisfactory level, enabling problem-free use of services. Packet loss are so "low" level, they are not felt by the user.

This article confirms that a dynamically developing new techniques and technologies are solutions ensuring network reliability. Thus, the presented network architecture using BYOD model is a very good example of this. As a result, users can use private mobile devices e.g. in the workplace, and use them to carry out tasks. And the employer can expect that the employee will work effectively, safely and reliably (in terms software and hardware oriented).

6. References

[1] https://technet.microsoft.com/en-us/library/dn528861.aspx (avb: VI.2016).
[2] https://www.ibm.com/mobilefirst/us/en/bring-your-own-device/byod.html (avb: 17.06.2016).
[3] Laskowski D., Stąpór P.: Bring Your Own Device – model bezpiecznego i efektywnego dostępu do sieci teleinformatycznej. Modele inżynierii teleinformatyki - tom 10. Politechnika Koszalińska 2015.
[4] Laskowski D., Byłak M.: Diagnosis coding efficiency of network coding mechanism for wireless networks, Electrical Review, R. 89 9/2013, Sigma-Not, Warsaw, 2013, pp. 133-138, ISSN 0033-2097.
[5] Łubkowski P., Laskowski D.: Selected Issues of Reliable Identification of Object in Transport Systems Using Video Monitoring Services, Communication in Computer and Information Science, Springer International Publishing AG, Switzerland, Volume 471, 2014, pp. 59-68, ISSN 1865-0929, ISBN 978-3-662-45316-2 (Print), DOI 10.1007/978-3-662-45317-9_7, 2014.
[6] Łubkowski P., Laskowski D.: Test of the multimedia services implementation in in-formation and communication networks, Advances in Intelligent Systems and Computing, Springer International Publishing AG, Switzerland, Volume 286, 2014, pp. 325-332, ISSN 2194-5357, ISBN 978-3-319-07012-4 (Print), DOI 10.1007/978-3-319-07013-1_31.
[7] Laskowski D.: Reliability assessment of date transmission systems, Safety and Reliability Systems, Publishing and printing House of the Air Forces Institute of Technologies, Poland, Journal of KONBiN No 1(29), 2014, pp. 69-79, ISSN 2083-4608 (Online), ISSN 1895-8281 (Print), DOI: 10.2478/jok.
[8] Polak R., Laskowski D.: Reliability of routing protocols, Safety and Reliability Systems, Publishing and printing House of the Air Forces Institute of Technologies, Poland, Journal of KONBiN No 3(35), 2015, pp. 51-62, ISSN 1895-8281, ESSN 2083-4608, DOI: 10.1515/jok-2015-039.
[9] Laskowski D., Łubkowski P.: The factors determining the reliability of IT network administrator, Electrical Review, Volume 92, pp. 16-20, Sigma-Not, Poland, 1/2016, DOI: 10.15199/48.2016.01.04, ISSN 0033-2097

[10] Siergiejczyk M., Krzykowska K., Rosiński A.: Parameters analysis of satellite support system in air navigation, Advances in intelligent systems and computing, Springer International Publishing AG, Switzerland, Volume 1089, 2015, pp. 673-678.
[11] Siergiejczyk M., Krzykowska K., Rosiński A.: Reliability assessment of cooperation and replacement of surveillance systems in air traffic, Advances in intelligent systems and computing, Springer International Publishing AG, Switzerland, Volume 286, 2014, pp. 403-411.
[12] Siergiejczyk M., Krzykowska K., Rosiński A.: Reliability assessment of integrated airport surface surveillance system, Advances in intelligent systems and computing, Springer International Publishing AG, Switzerland, Volume 365, 2015, pp. 435-443.
[13] Siergiejczyk M., Paś J., Rosiński A.: Evaluation of safety of highway CCTV system's maintenance process, Communications in Computer and Information Science, Springer International Publishing AG, Switzerland, Volume 471, 2014, pp. 69-79.

Dariusz Laskowski DSc. Eng. *graduated from the Faculty of Electronics, Military University of Technology, where he now works. He is a multi-faceted analysis of the phenomena determining the correct implementation of services in heterogeneous systems and networks offering data transmission. The focus is on reliability, safety, quality and survival of technical objects in terms of their practical use in heterogeneous networks (Share 50%).*

Paweł Stąpór MSc. *graduated from the Faculty of Electronics, Military University of Technology. He is interested in IT networks, particularly mobile networks and new technological solutions. Mainly focused on safety, reliability and quality of access to network resources from different locations (Share 50%).*

BRING YOUR OWN DEVICE - NIEZAWODNY MODEL DOSTĘPU DO DANYCH

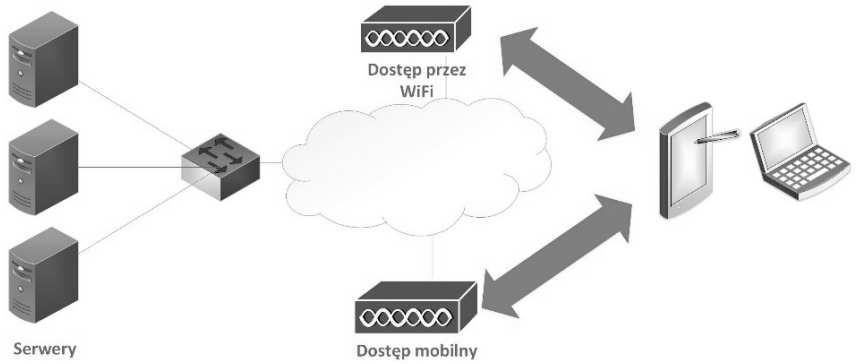
1. Wstęp

Ostatnie lata to okres dynamicznego rozwoju technologii i innowacji. To także okres, w którym nowsze rozwiązania technologiczne są „bardziej" osiągalne dla ludzi, a urządzenia przez nich użytkowane dysponują zaawansowanymi i wyszukanymi funkcjami. Obecnie, w dobie smartfonów oraz tabletów i powszechnego dostępu do Internetu, telefon komórkowy przejął większość funkcji komputera, a także posiada takie, które ułatwiają realizację różnych zadań. Według raportu Polska.Jest.Mobi 2015 przygotowanego we współpracy z TNS Polska w maju 2015 roku prawie 19 milionów smartfonów jest użytkowanych przez Polaków w wieku 15+, tj. 58% polskiego społeczeństwa. Użytkownicy wykorzystują swoje urządzenia mobilne tj. laptopy, tablety czy smatfony do różnych zadań. Pojawiła się nawet idea, aby pracownicy mogli używać swoje prywatne urządzenia w miejscu pracy, do realizacji powierzonych im zadań. Pomysł ten powstał, ponieważ zauważono, że pracownicy posiadają urządzenia, które są nowocześniejsze i bardziej wydajne niż te oferowane im przez pracodawcę. W związku z tym powstała koncepcja modelu Bring Your Own Device (BYOD) [1][2]. To dynamicznie rozwijane rozwiązanie jest wdrażane w różnych dziedzinach przez różnych dostawców świadczących usługi w obszarze teleinformatyki [10,11,12]. Poniższa publikacja jest sprawdzeniem niezawodności przedstawionej propozycji implementacji modelu BYOD, zapewniającym użytkownikowi dostęp do danych na wymaganym poziomie jakości.

2. Charakterystyka modelu BYOD

Bring Your Own Device jest to model umożliwiający użytkownikowi realizację zadań niezależnie od miejsca dyslokacji i uwarunkowań sieciowych, przy wykorzystaniu prywatnych urządzeń [3]. Model BYOD powinien oferować użytkownikowi dostęp bezprzewodowy (mobilny) a także przewodowy. Dostęp ten powinien być realizowany z wykorzystaniem najnowszych standardów. Bezprzewodową realizację obsługi użytkownika można podzielić na dwa sposoby [4]. Pierwszym z nich jest dostęp poprzez bezprzewodową sieć WLAN, z wykorzystaniem standardów 802.11n i 802.11ac/d poprzez punkt dostępowy w miejscu np. pracy. Drugim sposobem jest dostęp poprzez sieć mobilną (np. 3G/4G, WiMax, WiMax-2, LTE, LTE-A, itp.). Przewodowy dostęp może być realizowany z wykorzystaniem standardów FastEthernet czy GigiabitEthernet. Jedyną wadą tego modelu są niewłaściwe zabezpieczone urządzenia mobilne, a także możliwość nieprzestrzegania przez pracowników polityki bezpieczeństwa, ale to zdarzenie istnieje dla każdego rozwiązania sieciowego [5],[6].

Jak już wspomniano model BYOD ma szerokie zastosowanie i może być implementowany na wiele sposobów w zależności od zapotrzebowania. Ze względu na jego złożoność zaleca się przeprowadzenie analizy poszczególnych segmentów całego modelu. Ogólny model przestawiony poniżej (Rys. 1) można podzielić na 3 segmenty. Pierwszy z nich dotyczy miejsca gdzie przechowywane są dane bądź aplikacje z których użytkownik może zdalnie korzystać. Drugi segment to obszar realizacji routingu i dostępu do usługi. Obszar ten obejmuje infrastrukturę sieciową np. przedsiębiorstwa, architekturę dostawcy Internetu (ISP) oraz infrastrukturę dostępu do sieci – przewodowy lub mobilny. Trzeci segment to urządzenie użytkownika – specyfikacja urządzenia, metody zabezpieczenia, charakterystyka aplikacji sieciowej, itp. Każdy obszar można analizować pod różnymi kątami – bezpieczeństwa [13], efektywności, jakości QoS czy niezawodności.[7][8],[9] W poniższym artykule poddano analizie wszystkie obszary
i przeanalizowano je pod względem niezawodności.

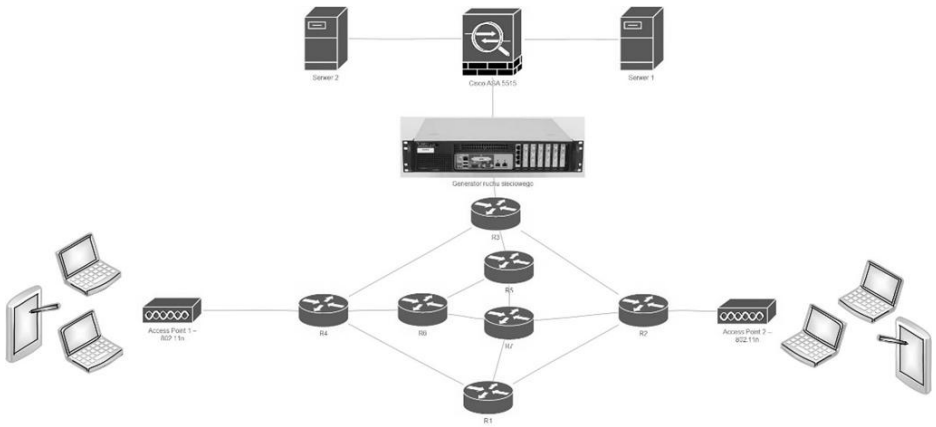


Rys. 1. Ogólna architektura modelu Bring Your Own Device.

3. Model badawczy

Model badawczy przedstawiono poniżej (Rys. 2). Do konfiguracji badanej sieci teleinformatycznej użyto powszechnie użytkowane urządzenia sieciowe, z których ważniejsze to: routery Cisco rodziny 28XX i 29XX, 24 portowe przełączniki 3COM rodziny Baseline 22XX, routery bezprzewodowe Cisco Small Bussiness WRVS4400N oraz dwa serwery Hewlett-Packard rodziny Proliant DL 360 generation 5 z Windows Serwer 2012 R2 ze skonfigurowanymi usługami m.in. Active Directory, DNS i Work Folders itp.
Poufność komunikacja osiągnięto poprzez tunele VPN wykorzystujące protokół SSLv3.0. Architektura ta zapewnia użytkownikowi dostęp przewodowy i mobilny. Na urządzeniu klienta zainstalowany został system operacyjny Windows 10, a przewodowa komunikacja z siecią odbywała się przez interfejs sieciowy standardu Gigabit Ethernet, natomiast bezprzewodowa z wykorzystaniem interfejsu standardu 802.11n.

W sieci uruchomiono routing z wykorzystaniem protokołu OSPF, natomiast urządzenia były zaadresowane z wykorzystaniem adresów IPv4. Jako usługę sieciową wykorzystano Work Folders. Usługa folderów roboczych umożliwia synchronizację plików pomiędzy serwerem a użytkownikami. Zasada działania jest zbliżona do takich aplikacji jak OneDrive czy Dropbox. Różnica polega na tym, że w przypadku tej usługi dane przechowywane są na serwerze lokalnym a nie na serwerze należącym do osób trzecich. Do uwierzytelniania wymagane jest konto i hasło domenowe. Work Folders używa protokołu HTTPS wraz z certyfikatem SSL do zapewnienia poufności danych.



Rys. 2. Architektura badawcza modelu BYOD

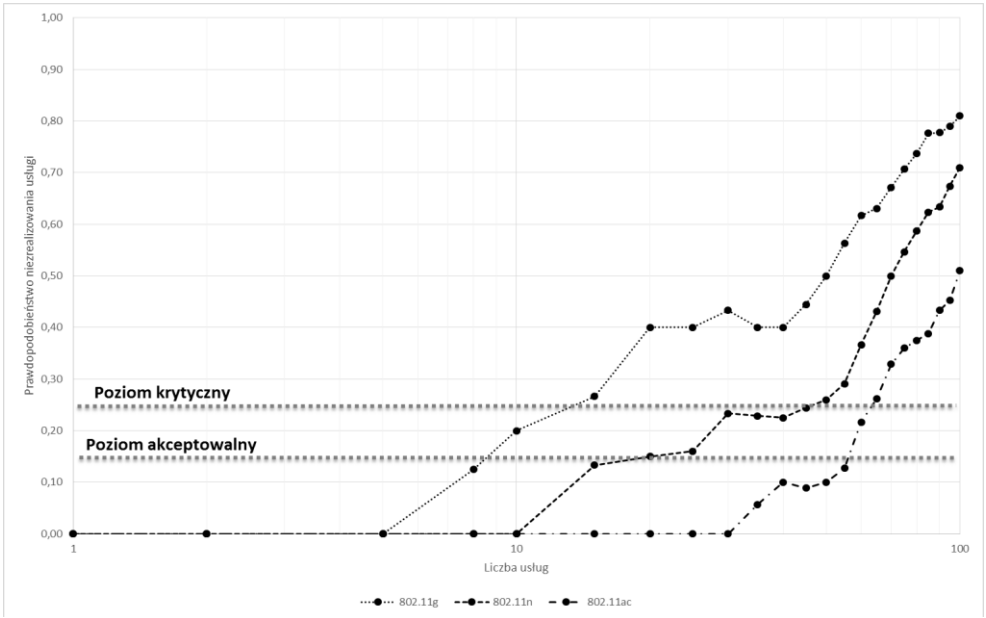
Administrator serwera może usuwać pliki znajdujące się w folderze roboczym użytkownika, a także zabezpieczyć je w taki sposób, aby zminimalizować ryzyko użycia plików w niepowołany sposób.[3] W modelu badawczym umieszczono także urządzenie emulujące ruch sieciowy – LANforge ICE CT50. Dodatkowo w badaniu wykorzystano kilka dodatkowych urządzeń mobilnych, tak, aby uzyskać dodatkowe obciążenie punktów dostępowych.

Na powyższym modelu BYOD przeprowadzono następujące badania:

- Zbadano prawdopodobieństwo niezrealizowania usługi w zależności od liczby uruchomionych usług w sieci. Liczbę usług zwiększano od 1 do 100. Dla każdego przypadku wykonano 80 powtórzeń, aby otrzymać jak najwiarygodniejsze wyniki. Jako limit czasowy zrealizowania usługi przyjęto 60 sekund. Badania przeprowadzono dla trzech standardów sieci bezprzewodowych: 802.11g, 802.11n i 802.11ac.
- Zbadano przepustowość i zmienność opóźnienia sieci dla użytkownika mającego dostęp do sieci z wykorzystaniem standardu 802.11n. Wykorzystujące wyniki z poprzedniego badania, przyjęto, że badanie zostanie przeprowadzone dla sieci, w której jest uruchomionych 10 usług. Dodatkowo przebadano sieć pod kątem strat pakietów w funkcji czasu.

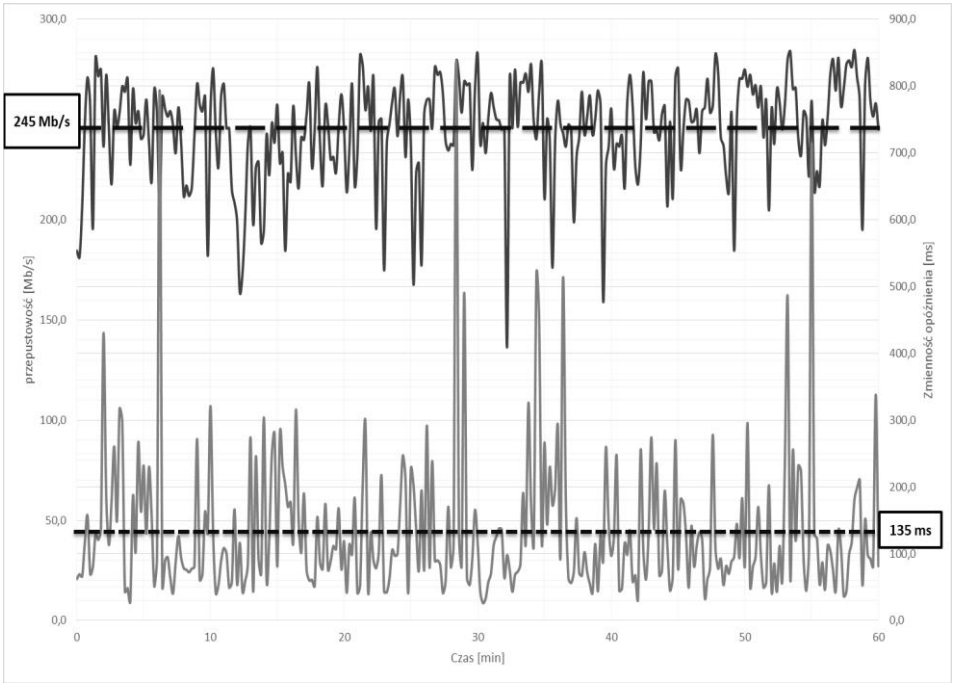
4. Wyniki badań i ich analiza

Na podstawie przeprowadzonych badań i otrzymanych wyników sporządzono wykresy prawdopodobieństwa niezrealizowania usługi w zależności od liczby uruchomionych usług (Rys. 6). Prawdopodobieństwo niezrealizowania usługi zostało wyliczone jako stosunek liczby niezrealizowanych usług do liczby zgłoszenia zapotrzebowania na usługę, tj 80 powtórzeń. Dla tego prawdopodobieństwa wyznaczono subiektywnie poziom dopuszczalny i krytyczny. Wyniósł on odpowiednio 0,15 – poziom dopuszczalny, 0,25 – poziom krytyczny.
Jak można zauważyć na wykresie (Rys. 7), najlepsze wyniki uzyskano dla standardu 802.11ac. Prawdopodobieństwo zaczęło rosnąć dopiero przy uruchomionych 35 usługach w sieci jednocześnie, podczas gdy dla standardu 802.11g było to 8 usług. Daje to ponad czterokrotnie wyższą niezawodność sieci. Oznacza to także, że wykorzystując najnowszy standard WiFi z sieci jednocześnie może korzystać czterokrotnie więcej użytkowników. Można więc stwierdzić, że wprowadzając nowsze standardy, a co za tym idzie wyższe przepustowości w sieci, zapewniamy większą niezawodność sieci oraz dostępu do zasobów sieciowych. Warto też zauważyć, że prawdopodobieństwo dla tych trzech standardów nie osiąga poziomu powyżej 0,8 (standard 802.11g). Oznacza to, że zawsze istnieje prawdopodobieństwo, że nasze zapotrzebowanie na usługę zostanie zrealizowane nawet przy bardzo obciążonej sieci.



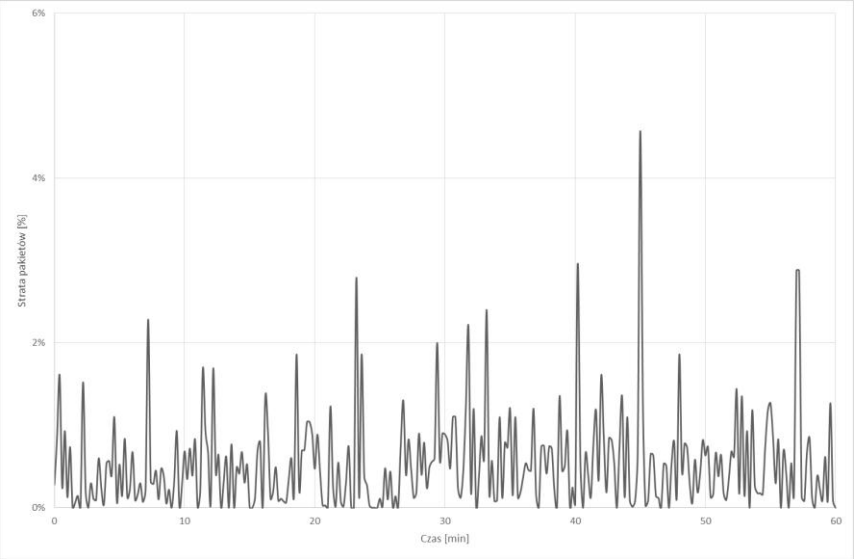
Rys. 3. Prawdopodobieństwo niezrealizowania usługi w zależności od liczby usług

Następnie zbadano sieć pod względem przepustowości i zmienności opóźnienia. W tym celu wykorzystano program IPerf. Na podstawie otrzymanych wyników sporządzono poniższy wykres (Rys. 4).



Rys. 4. Przepustowość i zmienność opóźnienia sieci w funkcji czasu dla standardu 802.11n

Średnia przepustowość dla standardu 802.11n wyniosła 245 Mb/s. Jest to dość zadowalający wynik, zwłaszcza, że w tym samym czasie z sieci korzystało 10 użytkowników. Jitter na średnim poziomie 135 ms jest wartością do zaakceptowania dla tej sieci. Maksymalne wartości w przedziale 300 – 850 ms, były chwilowe i w rzeczywistości nie zauważalne dla użytkownika. W tej sieci zmienność opóźnienia nie ma znaczącego wpływu na jakość obsługi, ponieważ sieć nie jest wykorzystywana do przesyłania pakietów w czasie rzeczywistym, tzn. nieobsługiwana jest telefonia internetowa VoIP czy transmisja strumieniowa wideo. Ostatnim badaniem było przebadanie sieci wykorzystującej model BYOD pod kątem strat pakietów. Uzyskane wyniki zaprezentowano na wykresie (Rys. 8). Czas obserwacji wynosił 60 minut, aby dokładniej zobrazować sytuację w sieci, a tym samym uzyskać obiektywniejsze wyniki. Jak można zauważyć, średni poziom strat pakietów nie przekracza 1%, co jest wynikiem bardzo zadowalającym. Chwilowe wyższe wartości strat pakietów były spowodowane większym natężeniem ruchu w sieci. Nie wpłynęło to w znaczący sposób na użytkowanie usługi, zapewniając tym samym niezawodną obsługę.



Rys. 5. Straty pakietów w sieci w funkcji czasu

5. Wnioski

W artykule przebadano model BYOD pod względem niezawodnego dostępu do zasobów sieciowych z wykorzystaniem standardów mobilnych. Przedstawione wyniki badań pokazują, że w zależności od zastosowanego standardu sieci bezprzewodowych sieć jest w stanie obsłużyć użytkownika z prawdopodobieństwem zależnym od liczby jednocześnie uruchomionych usług sieciowych. Użytkownik korzystający z usług modelu BYOD ma zapewniony niezawodny dostęp do zasobów sieciowych z przepustowością i zmiennością opóźnienia na zadowalającym poziomie, umożliwiającym bezproblemowe korzystanie z usług. Straty pakietów są na tyle „niskim" poziomie, że nie są odczuwalne przez użytkownika.

Powyższy artykuł potwierdza, że dynamicznie rozwijające się nowe techniki i technologie są rozwiązaniami zapewniającymi niezawodność sieci. Przedstawiona tutaj architektura sieci z wykorzystaniem modelu BYOD jest tego bardzo dobrym przykładem. Dzięki temu, użytkownicy mogą wykorzystywać prywatne urządzenia mobilne np. w miejscu pracy, i używać ich do realizacji zadań. A pracodawca może oczekiwać, że jego pracownik będzie pracował efektywnej, bezpiecznie i niezawodnie (pod względem software'owym i hardware'owym).

6. Literatura

[1] https://technet.microsoft.com/en-us/library/dn528861.aspx (osiągalna: 17.06.2016).
[2] https://www.ibm.com/mobilefirst/us/en/bring-your-own-device/byod.html (osiągalna: 17.06.2016).

[3] Laskowski D., Stąpór P.: Bring Your Own Device – model bezpiecznego i efektywnego dostępu do sieci teleinformatycznej. Modele inżynierii teleinformatyki - tom 10. Politechnika Koszalińska 2015.
[4] Laskowski D., Byłak M.: Diagnosis coding efficiency of network coding mechanism for wireless networks, Electrical Review, R. 89 9/2013, Sigma-Not, Warszawa, 2013r., str. 133-138, ISSN 0033-2097.
[5] Łubkowski P., Laskowski D.: Selected Issues of Reliable Identification of Object in Transport Systems Using Video Monitoring Services, Communication in Computer and Information Science, Springer International Publishing AG / Springer Berlin Heidelberg, Switzerland, Volume 471, 2014, pp 59-68, ISSN 1865-0929, ISBN 978-3-662-45316-2 (Print) 978-3-662-45317-9 (Online), DOI 10.1007/978-3-662-45317-9_7, 2014.
[6] Łubkowski P., Laskowski D.: Test of the multimedia services implementation in in-formation and communication networks, Advances in Intelligent Systems and Computing, Springer International Publishing AG, Switzerland, Volume 286, 2014, pp 325-332, ISSN 2194-5357, ISBN 978-3-319-07012-4 (Print) 978-3-319-07013-1(Online), DOI 10.1007/978-3-319-07013-1_31.
[7] Laskowski D.: Reliability assessment of date transmission systems, Safety and Reliability Systems, Publishing and printing House of the Air Forces Institute of Technologies, Poland, Journal of KONBiN No 1(29) 2014, pp.69-79, ISSN (Online) 2083-4608, ISSN (Print) 1895-8281, DOI: 10.2478/jok.
[8] Polak R., Laskowski D.: Reliability of routing protocols, Safety and Reliability Systems, Publishing and printing House of the Air Forces Institute of Technologies, Poland, Journal of KONBiN No 3(35) 2015, pp. 51-62, ISSN 1895-8281, ESSN 2083-4608, DOI: 10.1515/jok-2015-039.
[9] Laskowski D., Łubkowski P.: The factors determining the reliability of IT network administrator, Electrical Review, vol. 92, pp. 16-20, Sigma-Not, Poland, 1/2016, DOI: 10.15199/48.2016.01.04, ISSN 0033-2097
[10] Siergiejczyk M., Krzykowska K., Rosiński A.: Parameters analysis of satellite support system in air navigation. In: „Proceedings of the Twenty-Third International Conference on Systems Engineering", editors: H. Selvaraj, D. Zydek, G. Chmaj, given as the monographic publishing series – „Advances in intelligent systems and computing", Vol. 1089, pp. 673-678, Springer 2015.
[11] Siergiejczyk M., Krzykowska K., Rosiński A.: Reliability assessment of cooperation and replacement of surveillance systems in air traffic. In: „Proceedings of the Ninth International Conference Dependability and Complex Systems DepCoS-RELCOMEX", editors: Zamojski W., Mazurkiewicz J., Sugier J., Walkowiak T., Kacprzyk J., given as the monographic publishing series – „Advances in intelligent systems and computing", Vol. 286, pp. 403–411, Springer 2014.
[12] Siergiejczyk M., Krzykowska K., Rosiński A.: Reliability assessment of integrated airport surface surveillance system. In: „Proceedings of the Tenth International Conference on Dependability and Complex Systems DepCoS-RELCOMEX", editors: Zamojski W., Mazurkiewicz J., Sugier J., Walkowiak T., Kacprzyk J., given as the monographic publishing series – „Advances in intelligent systems and computing", Vol. 365, pp. 435-443. Springer, 2015.

[13] Siergiejczyk M., Paś J., Rosiński A.: Evaluation of safety of highway CCTV system's maintenance process. In: the monograph „Telematics – support for transport", editors: Mikulski J., given as the monographic publishing series – „Communications in Computer and Information Science", Vol. 471, pp. 69-79, Springer-Verlag, Berlin Heidelberg 2014.
[14] Choromański W., Dyduch J., Paś J.: „Minimizing the Impact of Electromagnetic Interference Affecting the Control System of Personal Rapid Transit in the Context of the Competitiveness of the Supply Chain" Archives Of Transport, Polish Academy of Sciences Index 201 901 ISSN 0866-9546 Volume 23, Issue 2, pp. 137-152, Warsaw 2011.

Dr hab. inż. Dariusz Laskowski *jest absolwentem wydziału Elektroniki Wojskowej Akademii Technicznej, gdzie obecnie pracuje. Zajmuje się wieloaspektową analizą zjawisk wpływających na prawidłową realizację usług w systemach i sieciach heterogenicznych oferujących transmisję danych. Koncentruje się na niezawodności, bezpieczeństwie, jakości oraz przetrwaniu obiektów technicznych pod kątem ich praktycznego zastosowania w sieciach heterogenicznych (Udział 50%).*

Mgr inż. Paweł Stąpór *jest absolwentem Wydziału Elektroniki Wojskowej Akademii Technicznej. Interesuje się sieciami teleinformatycznymi, w szczególności sieciami mobilnymi oraz nowymi rozwiązaniami technologicznymi. Głównie koncentruje się na bezpieczeństwie. Niezawodności i jakości dostępu do zasobów sieciowych z różnych lokalizacji (Udział 50%).*