DOKUMENTACJA POWYKONAWCZA

INWESTYCJA:	**Wdrożenia sieci LAN i WIFI w Wojewódzkim Szpitalu specjalistycznym nr 4 w Bytomiu**
LOKALIZACJA:	**Wojewódzki Szpital Specjalistyczny nr w Bytomiu** **Bytom, ul. Legionów 10**
TEMAT:	**Wdrożenia sieci WIFI oraz LAN w ramach projektu Zapewnienie rozwoju elektronicznych usług publicznych poprzez zakup i wdrożenie systemu informatycznego w Wojewódzkim Szpitalu Specjalistycznym nr 4 w Bytomiu**
STADIUM:	**DOKUMENTACJA POWYKONAWCZA**
WŁAŚCICIEL:	**Wojewódzki Szpital Specjalistyczny nr w Bytomiu**
JEDNOSTKA OPRACOWUJACA:	**Netology Sp z o.o.**
OPRACOWAŁ:	Kazimierz Gajczak. Michal Strzempa

KATOWICE – Maj 2015 r.

1. Wstęp.....3

2. Podstawa opracowania....3
3. Przedmiot oraz zakres opracowania....3
4. Opis techniczny sieci LAN....4
4.1 Topologia sieci LAN....4
4.1.1 Topologia fizyczna sieci....4
4.1.2 Topologia logiczna sieci....6
4.2 Wykaz urządzeń....8
5. Konfiguracja....13
5.1 VLAN....13
5.2 Adresacja IP w poszczególnych segmentach sieci....13
5.3 ACL....14
5.4 DHCP - konfiguracja dynamicznego przydzielania adresów IP dla poszczególnych podsieci....14
5.5 Zapobieganie pętlom w sieci – protokół STP....15
5.6 Routing w sieci....16
5.7 Ograniczenie dostępu do innych podsieci – listy ACL....17
6. Sieć bezprzewodowa....19
6.1 Opis budowy sieci WIFI....19
6.2 Wykaz urządzeń wchodzących w skład sieci WIFI....20
6.3 Wykaz sieci WLAN....22
6.4 Zarządzanie dostępem do sieci WIFI – autentykacja na serwerze Radius....22
6.4.1 Konfiguracja serwera Radius na kontrolerze WiFi....22
7. Opis serwera Autentykacji AGILE....25
8. Czynności serwisowe....25
8.1 Zarzadzanie konfiguracją....25
8.2 Konfiguracja VLAN....26
8.3 Backup / odtwarzanie konfiguracji....28
9. Hasła....28

1. Wstęp

Rozwiązania zawarte w niniejszej dokumentacji stanowią własność Wykonawcy i mogą być stosowane jedynie w celu określonym umową zawartą między Wykonawcą i Zamawiającym.

- Rysunki i część opisowa są w dokumentacji wzajemnie uzupełniającymi się. Wszystkie elementy ujęte w części opisowej, a nie pokazane na rysunkach oraz pokazane na rysunkach, a nie ujęte dokumentacją winny być traktowane jakby były ujęte w obu.

2. Podstawa opracowania

Podstawą niniejszego opracowania stanowią:

- Uzgodnienia z Inwestorem
- Projekt Wykonawczy
- Uzgodnienia międzybranżowe podczas wykonywania inwestycji
- Zasady współczesnej wiedzy technicznej

3. Przedmiot oraz zakres opracowania

Celem projektu w zakresie sieciowej było dostarczenie, montaż i konfiguracja urządzeń sieciowych pozwalających na zbudowanie niezawodnej sieci transmisji danych na potrzeby wdrożenia zamówienia na „Zapewnienie rozwoju elektronicznych usług publicznych poprzez zakup i wdrożenie systemu informatycznego w Wojewódzkim Szpitalu Specjalistycznym nr 4 w Bytomiu

W skład wdrożonej infrastruktury sieciowej wchodzą:

- infrastruktura kablowa w postaci okablowania optycznego i miedzianego do połaczeń fizycznych między urządzeniami sieciowymi oraz pomiędzy urządzeniami sieciowymi dostępowymi i urządzeniami końcowymi sieci (komputery, drukarki itp.)
- urządzenia sieciowe rdzeniowy i dystrybucyjne (switche modułowe L3) w centralnych punktach dystrybucyjnych ,
- urządzenia dostępowe sieci LAN w lokalnych punktach dystrybucyjnych PD (switche dostępowe L2),
- punkty dostępowe wifi rozmieszczone na terenie całego szpitala na korytarzach
- serwer zarządzający dostępem do sieci WIFI znajdujący się w serwerowni głównej jako maszyna wirtualna środowiska wirtualnego wdrażanego w ramach całego projektu.

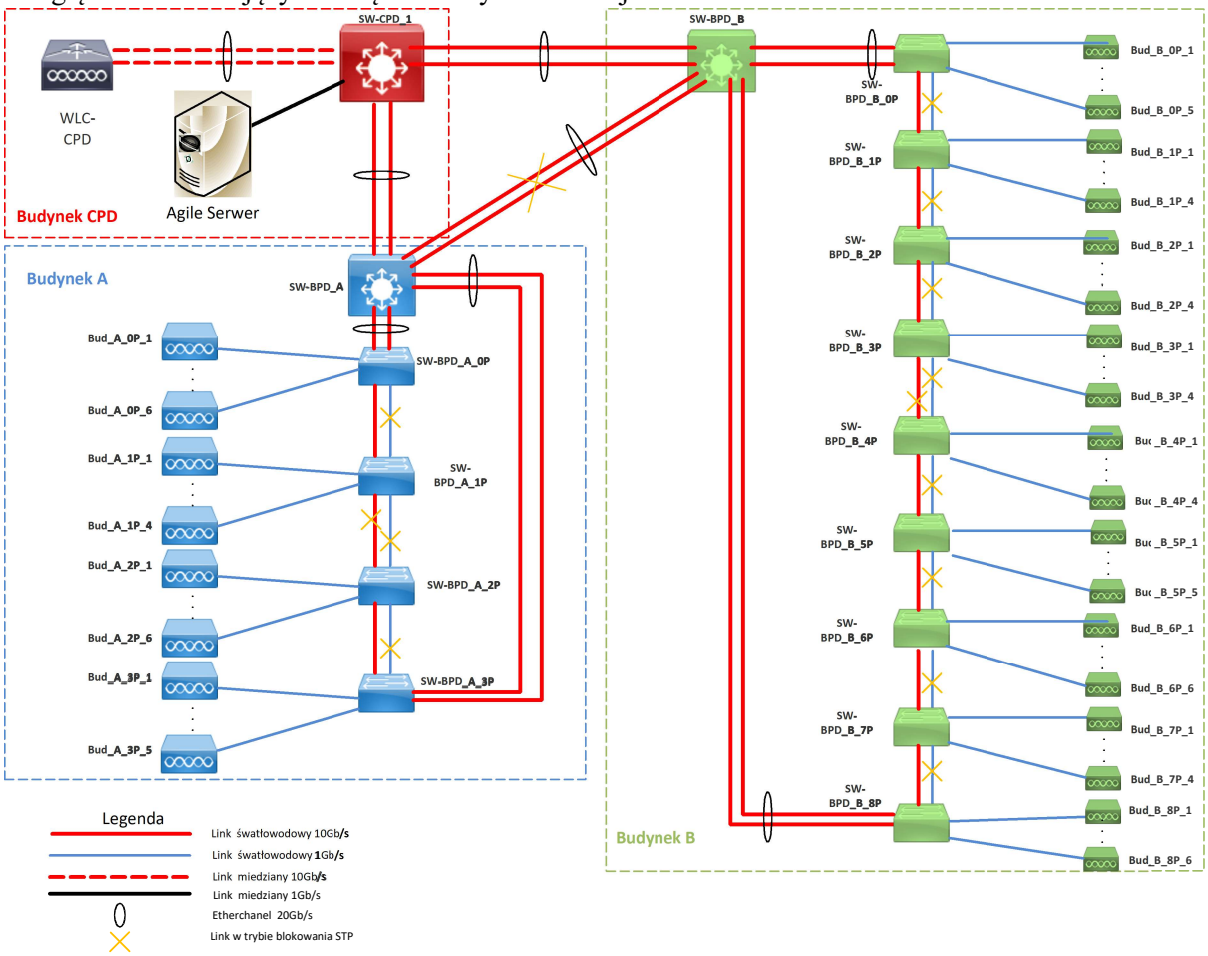
Niniejsze opracowanie opisuje budowę logiczną sieci, konfigurację urządzeń, schemat połączeń fizycznych między urządzeniami sieciowymi, wykaz urządzeń sieciowych oraz opis konfiguracji urządzeń w najczęściej używanych obszarach.

4. Opis techniczny sieci LAN

4.1 Topologia sieci LAN

4.1.1 Topologia fizyczna sieci

Poniższy rysunek przedstawia fizyczna topologię sieci w oparciu o wdrażane urządzenia sieciowe bez uwzględniania istniejących urządzeń dotychczasowej sieci



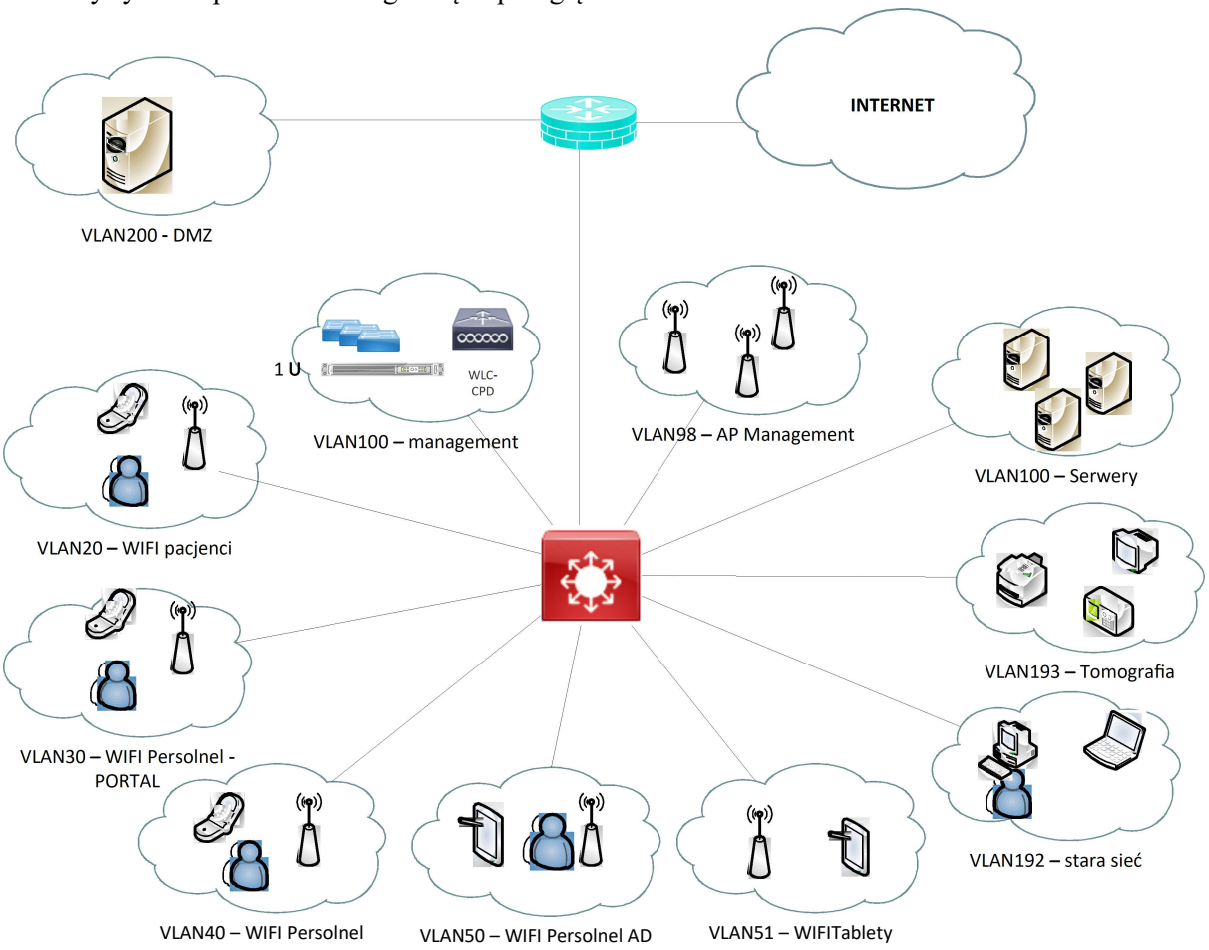
Rysunek 1. Topologia fizyczna sieci

Fizycznie sieć została zbudowana w topologii okręgów, w których główny switch rdzeniowy CORE (SW-CPD-1) , switch dystrybucyjny w budynkach A (SW-BPD_A) i switch dystrybucyjny w budynku B (SW-BPD_B) tworzą główny ring dystrybucyjny, a switche dostępowe wraz ze switchem dystrybucyjnym w budynkach A i B tworzą lokalne ringi lokalne.
Połączenia między switchami są zestawione za pomocą linków światłowodowych w wykorzystaniem światłowodów wielomodowych i modułów SFP (1Gb/s) i SFP+ (10Gb/s) w switchach.
W celu zapewnienia redundancji połączeń switche są połączone parą linków światłowodowych, przy czym połaczenia ze switchami dystrybucyjnymi są wszystkie w technologii SFP+ z szybkością 10Gb/s, a połaczenia między switchami dostępowymi w ringu są po jednym w technologii SFP (1Gb/s) i SFP+ (10Gb/s)
Dodatkowo połączenia fizyczne ze switchami dystrybycyjnymi są połaczone w logiczne linki agregujące, zwiększając przepustowość takiego linku do 20Gb/s i zapewniają pracę linku w razie awarii jednego z połączeń fizycznych
Do switchy dystrybycyjnych są podłączone punkty dostępowe AP, które są zarządzane poprzez

kontroler WIFI podłączony w głównej serwerowni do głównego switcha CORE oraz serwer Agile odpowiadający za autentykację użytkowników w sieci WIFI.

4.1.2 Topologia logiczna sieci

Poniższy rysunek przedstawia logiczną topologię sieci.



Rysunek 2 Topologia logiczna sieci

Logicznie nowo budowana sieć składa się z:
- podsieci logicznych w postaci VLANów, w których są podłączone urządzenia zgodnie z ich funkcją,
- switcha centralnego CPD, będącego bramą dla poszczególnych vlanów i zapewniającego routing między poszczególnymi VLAN-nami oraz firewallem brzegowym będący stykiem z siecią internet
- kontrolera WIFI zarządzającego dystrybucją sieci WIFI przez punkty dostępowe AP
- serwera autentykacji dla zarządzania dostępem do sieci WIFI przez klientów mobilnych

Tabela 1 Wykaz VLAN-ów

VLAN ID	nazwa	przeznaczenie
20	WLAN-personel	WiFi dla personelu
30	WLAN-pacjenci	WiFi dla pacjentów
40	WLAN-Goscie	WiFi dla gości
50	VLAN50-WIDI-AD	WIFI dla urządzeń firmowych z autentykacją przez serwer domeny przez 802.1x
51	VLAN51-TABLETY	WIFI dedykowana dla tabletów medycznych
98	WLAN-AP-zarzadzanie	siec zarzadzajaca dla WIFI
99	Zarzadzanie	zarzadzanie urządzeń sieci, serwerów, UPS itp.
100	serwery	serwery aplikacyjne wewnętrzne
192	LAN-OLD	dotychczasowa sieć LAN

193	LAN_Tomografia	podsieć dla urządzeń tomografii komputerowej
200	DMZ	serwery aplikacyjne z dostępem z zewnątrz
254	Polaczenie-LAN-UTM	sieć połączeniowa pomiędzy switchem CORE a UTM/routerem brzegowym

4.2 Wykaz urządzeń

W tabelach poniżej zawarte zostały informację dotyczące:
- adresacji IP urządzeń sieciowych oraz fizycznej lokalizacji
- typów i wyposażenia urządzeń (numery seryjne, nazwy komponentów, opis)

Dane dostępowe (loginy i hasła) zostaną dostarczone w osobnym dokumencie.

Tabela 2 Lista adresów IP urządzeń i lokalizacja

Urządzenie	hostname	Adres IP zarządzania	lokalizacja	Konfiguracja poprzez
kontroler WiFi	WLC-CPD	10.10.99.10	Budynek K serwerownia CPD	ssh, https
switch dystyrybucyjny CORE	SW-CPD-1	10.10.99.1	Budynek K serwerownia CPD	ssh, https
switch dystrybucyjny	SW-BPD_A3	10.10.99.20	Budynek A3 - poziom -1	ssh, https
switch dostępowy	SW-BPD_A3_0P	10.10.99.21	Budynek A3 - poziom -1	ssh, https
switch dostępowy	SW-BPD_A3_1P	10.10.99.22	Budynek A3 - poziom 1	ssh, https
switch dostępowy	SW-BPD_A3_2P	10.10.99.23	Budynek A3 - poziom 2	ssh, https
switch dostępowy	SW-BPD_A3_3P	10.10.99.24	Budynek A3 - poziom 3	ssh, https
switch dystrybucyjny	SW-BPD_B	10.10.99.30	Budynek B - poziom -1	ssh, https
switch dostępowy	SW-BPD_B_0P	10.10.99.31	Budynek B - poziom 0	ssh, https
switch dostępowy	SW-BPD_B_1P	10.10.99.32	Budynek B - poziom 1	ssh, https
switch dostępowy	SW-BPD_B_2P	10.10.99.33	Budynek B - poziom 2	ssh, https
switch dostępowy	SW-BPD_B_3P	10.10.99.34	Budynek B - poziom 3	ssh, https
switch dostępowy	SW-BPD_B_4P	10.10.99.35	Budynek B - poziom 4	ssh, https
switch dostępowy	SW-BPD_B_5P	10.10.99.36	Budynek B - poziom 5	ssh, https
switch dostępowy	SW-BPD_B_6P	10.10.99.37	Budynek B - poziom 6	ssh, https
switch dostępowy	SW-BPD_B_7P	10.10.99.38	Budynek B - poziom 7	ssh, https
switch dostępowy	SW-BPD_B_8P	10.10.99.39	Budynek B - poziom 8	ssh, https
UPS zasilający switch dystrybucyjny	Ups_03	10.10.99.41	Budynek A3 - poziom -1	http
UPS zasilający switch dystrybucyjny	Ups_04	10.10.99.42	Budynek B - poziom -1	http
UPS - moduł LAN	UPS_BPD_A_1P	10.10.99.43	Budynek A3 - poziom 1	http
UPS - moduł LAN	UPS_BPD_A_2P	10.10.99.44	Budynek A3 - poziom 2	http
UPS - moduł LAN	UPS_BPD_A_3P	10.10.99.45	Budynek A3 - poziom 3	http
UPS - moduł LAN	UPS_BPD_B_0P	10.10.99.46	Budynek B - poziom 0	http
UPS - moduł LAN	UPS_BPD_B_1P	10.10.99.47	Budynek B - poziom 1	http
UPS - moduł LAN	UPS_BPD_B_2P	10.10.99.48	Budynek B - poziom 2	http
UPS - moduł LAN	UPS_BPD_B_3P	10.10.99.49	Budynek B - poziom 3	http
UPS - moduł LAN	UPS_BPD_B_4P	10.10.99.50	Budynek B - poziom 4	http
UPS - moduł LAN	UPS_BPD_B_5P	10.10.99.51	Budynek B - poziom 5	http
UPS - moduł LAN	UPS_BPD_B_6P	10.10.99.52	Budynek B - poziom 6	http
UPS - moduł LAN	UPS_BPD_B_7P	10.10.99.53	Budynek B - poziom 7	http
UPS - moduł LAN	UPS_BPD_B_8P	10.10.99.54	Budynek B - poziom 8	http
Serwer AGILE	AGILE	10.10.100.10	Budynek K serwerownia CPD - VMWARE	https – serwer autentykacji RDP, VMWare vSphere – host

Tabela 3 Wykaz wyposażenia urządzeń

Nazwa sieciowa	TYP	Numer Seryjny	Opis

WLC-CPD	AC6605-26-PWR-16AP	210235791610EA000010	Assembling Components,AC6605-26-PWR-16AP,AC6605-26-PWR-16AP Bundle(Including AC6605-26-PWR,Resource License 16AP)
	W2PSA0500	21021309838NE7000160	AC/DC power module--25degC-55degC-90V-264V-12V/10A,-53.5V/7.1A
	W2PSA0500	21021309838NE7000131	AC/DC power module--25degC-55degC-90V-264V-12V/10A,-53.5V/7.1A
SW-CPD_1	ES0B07703	2102113304P0EC000469	Quidway S7703,ES0B07703,S7703 Assembly Chassis
	ES02G48VA	030KQT10EC000148	Quidway S7700,ES02G48VA,48-Port 10/100/1000BASE-T POE Interface Card(EA,RJ45,POE),32K MAC
	ES1D2X16SFC0	030PGP10F1000095	S7700,ES1D2X16SFC0,16-Port 10GBASE-X Interface Card(FC,SFP+) ,128K MAC
	ES02MCUA	030MPV10E5001420	Quidway S7700,ES02MCUA,Quidway S7703 Main Control Unit A
	ES0E2FBX	2102120760P0EC002254	Fan box,Quidway S7700,ES0E2FBX,Wide Voltage Fan Box
SW-BPD_A3	ES0B07703	2102113304P0EC000470	Quidway S7703,ES0B07703,S7703 Assembly Chassis
	ES02G48VA	030KQT10EC000154	Quidway S7700,ES02G48VA,48-Port 10/100/1000BASE-T POE Interface Card(EA,RJ45,POE),32K MAC
	ES1D2X16SFC0	030PGP10F1000096	S7700,ES1D2X16SFC0,16-Port 10GBASE-X Interface Card(FC,SFP+) ,128K MAC
	ES02MCUA	030MPV10E5001065	Quidway S7700,ES02MCUA,Quidway S7703 Main Control Unit A
	ES0E2FBX	2102120760P0EC002266	Fan box,Quidway S7700,ES0E2FBX,Wide Voltage Fan Box
SW-BPD_A3_0P	S5700-52X-PWR-LI-AC	210235421810EC000670	Assembling Components,S5700-52X-PWR-LI-AC,S5700-52X-PWR-LI-AC,S5700-52X-PWR-LI-AC(48 Ethernet 10/100/1000 PoE+ ports,4 10 Gig SFP+,AC 110/220V)
SW-BPD_A3_1P	S5700-52X-PWR-LI-AC	210235421810EC000667	Assembling Components,S5700-52X-PWR-LI-AC,S5700-52X-PWR-LI-AC,S5700-52X-PWR-LI-AC(48 Ethernet 10/100/1000 PoE+ ports,4 10 Gig SFP+,AC 110/220V)
SW-BPD_A3_2P	S5700-52X-PWR-LI-AC	210235421810EC000691	Assembling Components,S5700-52X-PWR-LI-AC,S5700-52X-PWR-LI-AC,S5700-52X-PWR-LI-AC(48 Ethernet 10/100/1000 PoE+ ports,4 10 Gig SFP+,AC 110/220V)
SW-BPD_A3_3P	S5700-52X-PWR-LI-AC	210235421810EC000689	Assembling Components,S5700-52X-PWR-LI-AC,S5700-52X-PWR-LI-AC,S5700-52X-PWR-LI-AC(48 Ethernet 10/100/1000 PoE+ ports,4 10 Gig SFP+,AC 110/220V)
SW-BPD_B	ES0B07703	2102113304P0EC000471	Quidway S7703,ES0B07703,S7703 Assembly Chassis
	ES02G48VA	030KQT10EC000147	Quidway S7700,ES02G48VA,48-Port 10/100/1000BASE-T POE Interface Card(EA,RJ45,POE),32K MAC
	ES1D2X16SFC0	030PGP10F1000094	S7700,ES1D2X16SFC0,16-Port 10GBASE-X Interface Card(FC,SFP+) ,128K MAC
	ES02MCUA	030MPV10E5001422	Quidway S7700,ES02MCUA,Quidway S7703 Main Control Unit A
	ES0E2FBX	2102120760P0EC002286	Fan box,Quidway S7700,ES0E2FBX,Wide Voltage Fan Box
SW-BPD_B_0P	S5700-52X-PWR-LI-AC	210235421810EC000676	Assembling Components,S5700-52X-PWR-LI-AC,S5700-52X-PWR-LI-AC,S5700-52X-PWR-LI-AC(48 Ethernet 10/100/1000 PoE+ ports,4 10 Gig SFP+,AC 110/220V)
SW-BPD_B_1P	S5700-52X-PWR-LI-AC	210235421810D9000051	Assembling Components,S5700-52X-PWR-LI-AC,S5700-52X-PWR-LI-AC,S5700-52X-PWR-LI-AC(48 Ethernet 10/100/1000 PoE+ ports,4 10 Gig SFP+,AC 110/220V)
SW-BPD_B_2P	S5700-52X-PWR-LI-AC	210235421810EC000682	Assembling Components,S5700-52X-PWR-LI-AC,S5700-52X-PWR-LI-AC,S5700-52X-PWR-LI-AC(48 Ethernet 10/100/1000 PoE+ ports,4 10 Gig SFP+,AC 110/220V)
SW-BPD_B_3P	S5700-52X-PWR-LI-AC	210235421810EC000690	Assembling Components,S5700-52X-PWR-LI-AC,S5700-52X-PWR-LI-AC,S5700-52X-PWR-LI-AC(48 Ethernet 10/100/1000 PoE+ ports,4 10 Gig SFP+,AC 110/220V)
SW-BPD_B_4P	S5700-52X-PWR-LI-AC	210235421810EC000675	Assembling Components,S5700-52X-PWR-LI-AC,S5700-52X-PWR-LI-AC,S5700-52X-PWR-LI-AC(48 Ethernet 10/100/1000 PoE+ ports,4 10 Gig SFP+,AC 110/220V)
SW-BPD_B_5P	S5700-52X-PWR-LI-AC	210235421810EC000669	Assembling Components,S5700-52X-PWR-LI-AC,S5700-52X-PWR-LI-AC,S5700-52X-PWR-LI-AC(48 Ethernet 10/100/1000 PoE+ ports,4 10 Gig SFP+,AC 110/220V)
SW-BPD_B_6P	S5700-52X-PWR-LI-AC	210235421810EC000674	Assembling Components,S5700-52X-PWR-LI-AC,S5700-52X-PWR-LI-AC,S5700-52X-PWR-LI-AC(48 Ethernet 10/100/1000 PoE+ ports,4 10 Gig SFP+,AC 110/220V)

SW-BPD_B_8P	S5700-52X-PWR-LI-AC	210235421810EC000684	Assembling Components,S5700-52X-PWR-LI-AC,S5700-52X-PWR-LI-AC,S5700-52X-PWR-LI-AC(48 Ethernet 10/100/1000 PoE+ ports,4 10 Gig SFP+,AC 110/220V)
SW-BPD_B_9P	S5700-52X-PWR-LI-AC	210235421810EC000668	Assembling Components,S5700-52X-PWR-LI-AC,S5700-52X-PWR-LI-AC,S5700-52X-PWR-LI-AC(48 Ethernet 10/100/1000 PoE+ ports,4 10 Gig SFP+,AC 110/220V)
Bud_A_0P_1	AP6010DN-AGN	2102354196W0EA001684	AP6010DN-AGN,AP6010DN-AGN Mainframe(11n,General AP Indoor,2x2 Double Frequency,Built-in Antenna,No AC/DC adapter)
Bud_A_0P_2	AP6010DN-AGN	2102354196W0EA001612	AP6010DN-AGN,AP6010DN-AGN Mainframe(11n,General AP Indoor,2x2 Double Frequency,Built-in Antenna,No AC/DC adapter)
Bud_A_0P_3	AP6010DN-AGN	2102354196W0EA001647	AP6010DN-AGN,AP6010DN-AGN Mainframe(11n,General AP Indoor,2x2 Double Frequency,Built-in Antenna,No AC/DC adapter)
Bud_A_0P_4	AP6010DN-AGN	2102354196W0EA001685	AP6010DN-AGN,AP6010DN-AGN Mainframe(11n,General AP Indoor,2x2 Double Frequency,Built-in Antenna,No AC/DC adapter)
Bud_A_0P_5	AP6010DN-AGN	2102354196W0EA001762	AP6010DN-AGN,AP6010DN-AGN Mainframe(11n,General AP Indoor,2x2 Double Frequency,Built-in Antenna,No AC/DC adapter)
Bud_A_0P_6	AP6010DN-AGN	2102354196W0EA001706	AP6010DN-AGN,AP6010DN-AGN Mainframe(11n,General AP Indoor,2x2 Double Frequency,Built-in Antenna,No AC/DC adapter)
Bud_A_1P_1	AP6010DN-AGN	2102354196W0EA001610	AP6010DN-AGN,AP6010DN-AGN Mainframe(11n,General AP Indoor,2x2 Double Frequency,Built-in Antenna,No AC/DC adapter)
Bud_A_1P_2	AP6010DN-AGN	2102354196W0EA001666	AP6010DN-AGN,AP6010DN-AGN Mainframe(11n,General AP Indoor,2x2 Double Frequency,Built-in Antenna,No AC/DC adapter)
Bud_A_1P_3	AP6010DN-AGN	2102354196W0EA001645	AP6010DN-AGN,AP6010DN-AGN Mainframe(11n,General AP Indoor,2x2 Double Frequency,Built-in Antenna,No AC/DC adapter)
Bud_A_1P_4	AP6010DN-AGN	2102354196W0EA001606	AP6010DN-AGN,AP6010DN-AGN Mainframe(11n,General AP Indoor,2x2 Double Frequency,Built-in Antenna,No AC/DC adapter)
Bud_A_2P_1	AP6010DN-AGN	2102354196W0E8000781	AP6010DN-AGN,AP6010DN-AGN Mainframe(11n,General AP Indoor,2x2 Double Frequency,Built-in Antenna,No AC/DC adapter)
Bud_A_2P_2	AP6010DN-AGN	2102354196W0E8000786	AP6010DN-AGN,AP6010DN-AGN Mainframe(11n,General AP Indoor,2x2 Double Frequency,Built-in Antenna,No AC/DC adapter)
Bud_A_2P_3	AP6010DN-AGN	2102354196W0E8000815	AP6010DN-AGN,AP6010DN-AGN Mainframe(11n,General AP Indoor,2x2 Double Frequency,Built-in Antenna,No AC/DC adapter)
Bud_A_2P_4	AP6010DN-AGN	2102354196W0E8000790	AP6010DN-AGN,AP6010DN-AGN Mainframe(11n,General AP Indoor,2x2 Double Frequency,Built-in Antenna,No AC/DC adapter)
Bud_A_2P_5	AP6010DN-AGN	2102354196W0E8000788	AP6010DN-AGN,AP6010DN-AGN Mainframe(11n,General AP Indoor,2x2 Double Frequency,Built-in Antenna,No AC/DC adapter)
Bud_A_2P_6	AP6010DN-AGN	2102354196W0E8000791	AP6010DN-AGN,AP6010DN-AGN Mainframe(11n,General AP Indoor,2x2 Double Frequency,Built-in Antenna,No AC/DC adapter)
Bud_A_3P_1	AP6010DN-AGN	2102354196W0EA001675	AP6010DN-AGN,AP6010DN-AGN Mainframe(11n,General AP Indoor,2x2 Double Frequency,Built-in Antenna,No AC/DC adapter)
Bud_A_3P_2	AP6010DN-AGN	2102354196W0EA001678	AP6010DN-AGN,AP6010DN-AGN Mainframe(11n,General AP Indoor,2x2 Double Frequency,Built-in Antenna,No AC/DC adapter)
Bud_A_3P_3	AP6010DN-AGN	2102354196W0E8000784	AP6010DN-AGN,AP6010DN-AGN Mainframe(11n,General AP Indoor,2x2 Double Frequency,Built-in Antenna,No AC/DC adapter)
Bud_A_3P_4	AP6010DN-AGN	2102354196W0E8000795	AP6010DN-AGN,AP6010DN-AGN Mainframe(11n,General AP Indoor,2x2 Double Frequency,Built-in Antenna,No AC/DC adapter)
Bud_A_3P_5	AP6010DN-AGN	2102354196W0E8000789	AP6010DN-AGN,AP6010DN-AGN Mainframe(11n,General AP Indoor,2x2 Double Frequency,Built-in Antenna,No AC/DC adapter)
Bud_B_0P_1	AP6010DN-AGN	2102354196W0E8000844	AP6010DN-AGN,AP6010DN-AGN Mainframe(11n,General AP Indoor,2x2 Double Frequency,Built-in Antenna,No AC/DC adapter)
Bud_B_0P_2	AP6010DN-AGN	2102354196W0E8001035	AP6010DN-AGN,AP6010DN-AGN Mainframe(11n,General AP Indoor,2x2 Double Frequency,Built-in Antenna,No AC/DC adapter)
Bud_B_0P_3	AP6010DN-AGN	2102354196W0E8000787	AP6010DN-AGN,AP6010DN-AGN Mainframe(11n,General AP Indoor,2x2 Double Frequency,Built-in Antenna,No AC/DC adapter)
Bud_B_0P_4	AP6010DN-AGN	2102354196W0E8001034	AP6010DN-AGN,AP6010DN-AGN Mainframe(11n,General AP Indoor,2x2 Double Frequency,Built-in Antenna,No AC/DC adapter)
Bud_B_0P_5	AP6010DN-AGN	2102354196W0E8001029	AP6010DN-AGN,AP6010DN-AGN Mainframe(11n,General AP Indoor,2x2 Double Frequency,Built-in Antenna,No AC/DC adapter)

Bud_B_1P_1	AP6010DN-AGN	2102354196W0E8001007	AP6010DN-AGN,AP6010DN-AGN Mainframe(11n,General AP Indoor,2x2 Double Frequency,Built-in Antenna,No AC/DC adapter)
Bud_B_1P_2	AP6010DN-AGN	2102354196W0E8001010	AP6010DN-AGN,AP6010DN-AGN Mainframe(11n,General AP Indoor,2x2 Double Frequency,Built-in Antenna,No AC/DC adapter)
Bud_B_1P_3	AP6010DN-AGN	2102354196W0E8001008	AP6010DN-AGN,AP6010DN-AGN Mainframe(11n,General AP Indoor,2x2 Double Frequency,Built-in Antenna,No AC/DC adapter)
Bud_B_1P_4	AP6010DN-AGN	2102354196W0E8001026	AP6010DN-AGN,AP6010DN-AGN Mainframe(11n,General AP Indoor,2x2 Double Frequency,Built-in Antenna,No AC/DC adapter)
Bud_B_2P_1	AP6010DN-AGN	2102354196W0E8001011	AP6010DN-AGN,AP6010DN-AGN Mainframe(11n,General AP Indoor,2x2 Double Frequency,Built-in Antenna,No AC/DC adapter)
Bud_B_2P_2	AP6010DN-AGN	2102354196W0E8001012	AP6010DN-AGN,AP6010DN-AGN Mainframe(11n,General AP Indoor,2x2 Double Frequency,Built-in Antenna,No AC/DC adapter)
Bud_B_2P_3	AP6010DN-AGN	2102354196W0EA001769	AP6010DN-AGN,AP6010DN-AGN Mainframe(11n,General AP Indoor,2x2 Double Frequency,Built-in Antenna,No AC/DC adapter)
Bud_B_2P_4	AP6010DN-AGN	2102354196W0E8001014	AP6010DN-AGN,AP6010DN-AGN Mainframe(11n,General AP Indoor,2x2 Double Frequency,Built-in Antenna,No AC/DC adapter)
Bud_B_3P_1	AP6010DN-AGN	2102354196W0EA001693	AP6010DN-AGN,AP6010DN-AGN Mainframe(11n,General AP Indoor,2x2 Double Frequency,Built-in Antenna,No AC/DC adapter)
Bud_B_3P_2	AP6010DN-AGN	2102354196W0E8000805	AP6010DN-AGN,AP6010DN-AGN Mainframe(11n,General AP Indoor,2x2 Double Frequency,Built-in Antenna,No AC/DC adapter)
Bud_B_3P_3	AP6010DN-AGN	2102354196W0EA001609	AP6010DN-AGN,AP6010DN-AGN Mainframe(11n,General AP Indoor,2x2 Double Frequency,Built-in Antenna,No AC/DC adapter)
Bud_B_3P_4	AP6010DN-AGN	2102354196W0EA001767	AP6010DN-AGN,AP6010DN-AGN Mainframe(11n,General AP Indoor,2x2 Double Frequency,Built-in Antenna,No AC/DC adapter)
Bud_B_4P_1	AP6010DN-AGN	2102354196W0E8001027	AP6010DN-AGN,AP6010DN-AGN Mainframe(11n,General AP Indoor,2x2 Double Frequency,Built-in Antenna,No AC/DC adapter)
Bud_B_4P_2	AP6010DN-AGN	2102354196W0E8001019	AP6010DN-AGN,AP6010DN-AGN Mainframe(11n,General AP Indoor,2x2 Double Frequency,Built-in Antenna,No AC/DC adapter)
Bud_B_4P_3	AP6010DN-AGN	2102354196W0E8001033	AP6010DN-AGN,AP6010DN-AGN Mainframe(11n,General AP Indoor,2x2 Double Frequency,Built-in Antenna,No AC/DC adapter)
Bud_B_4P_4	AP6010DN-AGN	2102354196W0E8001031	AP6010DN-AGN,AP6010DN-AGN Mainframe(11n,General AP Indoor,2x2 Double Frequency,Built-in Antenna,No AC/DC adapter)
Bud_B_5P_1	AP6010DN-AGN	2102354196W0E8000783	AP6010DN-AGN,AP6010DN-AGN Mainframe(11n,General AP Indoor,2x2 Double Frequency,Built-in Antenna,No AC/DC adapter)
Bud_B_5P_2	AP6010DN-AGN	2102354196W0E8000785	AP6010DN-AGN,AP6010DN-AGN Mainframe(11n,General AP Indoor,2x2 Double Frequency,Built-in Antenna,No AC/DC adapter)
Bud_B_5P_3	AP6010DN-AGN	2102354196W0E8000782	AP6010DN-AGN,AP6010DN-AGN Mainframe(11n,General AP Indoor,2x2 Double Frequency,Built-in Antenna,No AC/DC adapter)
Bud_B_5P_4	AP6010DN-AGN	2102354196W0E8000813	AP6010DN-AGN,AP6010DN-AGN Mainframe(11n,General AP Indoor,2x2 Double Frequency,Built-in Antenna,No AC/DC adapter)
Bud_B_5P_5	AP6010DN-AGN	2102354196W0E8000799	AP6010DN-AGN,AP6010DN-AGN Mainframe(11n,General AP Indoor,2x2 Double Frequency,Built-in Antenna,No AC/DC adapter)
Bud_B_6P_1	AP6010DN-AGN	2102354196W0E8001044	AP6010DN-AGN,AP6010DN-AGN Mainframe(11n,General AP Indoor,2x2 Double Frequency,Built-in Antenna,No AC/DC adapter)
Bud_B_6P_2	AP6010DN-AGN	2102354196W0E8001001	AP6010DN-AGN,AP6010DN-AGN Mainframe(11n,General AP Indoor,2x2 Double Frequency,Built-in Antenna,No AC/DC adapter)
Bud_B_6P_3	AP6010DN-AGN	2102354196W0E8000990	AP6010DN-AGN,AP6010DN-AGN Mainframe(11n,General AP Indoor,2x2 Double Frequency,Built-in Antenna,No AC/DC adapter)
Bud_B_6P_4	AP6010DN-AGN	2102354196W0EA001756	AP6010DN-AGN,AP6010DN-AGN Mainframe(11n,General AP Indoor,2x2 Double Frequency,Built-in Antenna,No AC/DC adapter)
Bud_B_6P_5	AP6010DN-AGN	2102354196W0EA001738	AP6010DN-AGN,AP6010DN-AGN Mainframe(11n,General AP Indoor,2x2 Double Frequency,Built-in Antenna,No AC/DC adapter)
Bud_B_6P_6	AP6010DN-AGN	2102354196W0E8001030	AP6010DN-AGN,AP6010DN-AGN Mainframe(11n,General AP Indoor,2x2 Double Frequency,Built-in Antenna,No AC/DC adapter)
Bud_B_7P_1	AP6010DN-AGN	2102354196W0E8001024	AP6010DN-AGN,AP6010DN-AGN Mainframe(11n,General AP Indoor,2x2 Double Frequency,Built-in Antenna,No AC/DC adapter)
Bud_B_7P_2	AP6010DN-AGN	2102354196W0E8001020	AP6010DN-AGN,AP6010DN-AGN Mainframe(11n,General AP Indoor,2x2 Double Frequency,Built-in Antenna,No AC/DC adapter)

Bud_B_7P_3	AP6010DN-AGN	2102354196W0E8001038	AP6010DN-AGN,AP6010DN-AGN Mainframe(11n,General AP Indoor,2x2 Double Frequency,Built-in Antenna,No AC/DC adapter)
Bud_B_7P_4	AP6010DN-AGN	2102354196W0E8001039	AP6010DN-AGN,AP6010DN-AGN Mainframe(11n,General AP Indoor,2x2 Double Frequency,Built-in Antenna,No AC/DC adapter)
Bud_B_8P_1	AP6010DN-AGN	2102354196W0EA001743	AP6010DN-AGN,AP6010DN-AGN Mainframe(11n,General AP Indoor,2x2 Double Frequency,Built-in Antenna,No AC/DC adapter)
Bud_B_8P_2	AP6010DN-AGN	2102354196W0EA001723	AP6010DN-AGN,AP6010DN-AGN Mainframe(11n,General AP Indoor,2x2 Double Frequency,Built-in Antenna,No AC/DC adapter)
Bud_B_8P_3	AP6010DN-AGN	2102354196W0EA001641	AP6010DN-AGN,AP6010DN-AGN Mainframe(11n,General AP Indoor,2x2 Double Frequency,Built-in Antenna,No AC/DC adapter)
Bud_B_8P_4	AP6010DN-AGN	2102354196W0EA001721	AP6010DN-AGN,AP6010DN-AGN Mainframe(11n,General AP Indoor,2x2 Double Frequency,Built-in Antenna,No AC/DC adapter)
Bud_B_8P_5	AP6010DN-AGN	2102354196W0EA001749	AP6010DN-AGN,AP6010DN-AGN Mainframe(11n,General AP Indoor,2x2 Double Frequency,Built-in Antenna,No AC/DC adapter)
Bud_B_8P_6	AP6010DN-AGN	2102354196W0EA001746	AP6010DN-AGN,AP6010DN-AGN Mainframe(11n,General AP Indoor,2x2 Double Frequency,Built-in Antenna,No AC/DC adapter)

5. Konfiguracja

W załączniku nr 1 dołaczono konfigurację urządzeń sieciowych (switche, kontroler WiFi)

5.1 VLAN

W poniższych punktach zawarto najważniejsze elementy konfiguracyjne podsieci VLAN rozgłaszanych przez switch rdzeniowy CORE Dla każdej z podsieci VLAN zdefiniowano adresy IP; W ostatnim punkcie zawarto sposób przeprowadzana najważniejszych czynności konfiguracyjnych dla podsieci VLAN

5.2 Adresacja IP w poszczególnych segmentach sieci

W poniższej tabeli zawarto zestawienie konfiguracji IP podsieci VLAN.
W załączniku nr 2 – plik zestawiono rezerwacje adresów IP we wszystkich podsieciach
Dla niektórych podsieci uruchomione przydzielanie adresów IP z serwerów DHCP

Tabela 4 Wykaz sieci VLAN wraz z adresacją

VLAN ID	nazwa	adresacja sieci	maska sieci	Brama sieci	Brama - urządzenie	Serwer DHCP
20	WLAN-personel	10.20.0.0	255.255.248.0	10.20.0.1	SW-CPD-1	WLC-CPD - 10.20.0.2
30	WLAN-pacjenci	10.30.0.0	255.255.248.0	10.30.0.1	SW-CPD-1	WLC-CPD - 10.30.0.2
40	WLAN-Goscie	10.40.0.0	255.255.248.0	10.40.0.1	SW-CPD-1	WLC-CPD - 10.40.0.2
50	VLAN50-WIDI-AD	10.50.0.0	255.255.255.0	10.50.0.1	SW-CPD-1	WLC-CPD - 10.50.0.2
51	VLAN51-TABLETY	10.50.1.0	255.255.255.0	10.50.1.1	SW-CPD-1	WLC-CPD - 10.50.1.2
98	WLAN-AP-zarzadzanie	10.10.98.0	255.255.255.0	10.10.98.1	SW-CPD-1	WLC-CPD - 10.10.98.1
99	Zarzadzanie	10.10.99.0	255.255.255.0	10.10.99.1	SW-CPD-1	SW-CPD-1 – 10.10.99.1
100	serwery	10.10.100.0	255.255.255.0	10.10.100.1	SW-CPD-1	Brak
192	LAN-OLD	192.168.0.0	255.255.248.0	192.168.3.100	SW-CPD-1	Relay 10.10.100.140
193	LAN_Tomografia	192.168.100.0	255.255.255.0	192.168.100.199	SW-CPD-1	Brak
200	DMZ	10.10.200.0	255.255.255.0	10.10.200.1	UTM-Netasq	brak
254	Polaczenie-LAN-UTM	10.10.254.0	255.255.255.0	10.10.254.1	SW-CPD-1	brak

5.3 ACL

Na potrzeby ograniczenia ruchu pomiędzy podsieciami VLAN na przełączniku rdzeniowym CORE SW-CPD-1 zostały skonfigurowane listy ACL ograniczające ruch pomiędzy poszczególnymi podsieciami.

Dodatkowo na kontrolerze WIFI zostały skonfigurowane listy ACL ograniczające ruch z poszczególnych klientów sieci WLAN do innych segmentów sieci, które są przypisywane dynamicznie przez serwer zarządzający dostępem WIFi – Agile.

Dostęp z i do vlan 200 (DMZ) jest terminowany przez firewall UTM Netasq, który jest bramą dla tej sieci i routuje ruch miedzy DMZ a pozostałymi sieciami.

Tabela 5 Konfiguracja list ACL na przełączniku rdzeniowym ACL

nazwa	opis	reguły
do_Oracle 3000	Ograniczenie ruchu z komputerów z VLAN192 do serwera Oracle	rule 5 permit tcp source 192.168.0.0 0.0.255.255 destination 10.10.100.100 0 destination-port eq 1521 rule 10 permit icmp source 192.168.0.0 0.0.255.255 destination 10.10.100.100 0 rule 20 permit tcp source 192.168.0.0 0.0.255.255 destination 10.10.100.100 0 destination-port eq 3389 rule 55 permit icmp source 192.168.0.0 0.0.255.255 rule 60 permit udp destination 10.10.100.100 0 destination-port eq ntp rule 65 permit udp destination 10.10.100.100 0 destination-port eq 563 rule 90 deny ip destination 10.10.100.100 0 rule 100 permit ip

Tabela 6 Konfiguracja list ACL na kontrolerze WIFI

nazwa	opis	reguły
acl number 3020	Ograniczenie ruchu klientów WIFI do pozostałych podsieci przypisaywane dynamicznie poszczególnym klientom WIFI przez serwera Agile podczas autentykacji w sieci	rule 5 permit tcp destination 192.168.2.106 0 destination-port eq domain rule 10 permit udp destination 192.168.2.106 0 destination-port eq dns rule 15 permit ip destination 10.10.100.10 0 rule 20 deny ip destination 192.168.0.0 0.0.255.255 rule 25 deny ip destination 10.0.0.0 0.255.255.255 rule 30 permit ip

5.4 DHCP - konfiguracja dynamicznego przydzielania adresów IP dla poszczególnych podsieci

Dla niektórych podsieci (VLANów) uruchomiono dynamiczne przydzielanie adresów IP przez serwer DHCP.

Dla klientów WIFI, serwerem DHCP jest kontroler WIFI , przydzielając adresy z poszczególnych vlanów adekwatnie do danego WLAN

Dla komputerów w sieci Stary_LAN zapytania DHCP są przekierowywane przez switch rdzeniowy (brama) do serwera domeny, który świadczy usługę serwera DHCP.

W VLANie managementowym 99, rolę serwera DHCP pełni switch rdzeniowy SW-CPD-1

W poniższej tabeli zestawiono parametry przydzielania adresów IP w poszczególnych VLANach

Tabela 7 Przydział adresów IP z DHCP

VLAN ID	Nazwa VLAN	Serwer DHCP	Zakres przydzielanych adresów IP	Serwery DNS przypisywane przez DHCP
20	WLAN-personel	WLC-CPD - 10.20.0.2	10.20.0.11-10.20.7.254	10.10.100.140, 8.8.8.8
30	WLAN-pacjenci	WLC-CPD - 10.30.0.2	10.30.0.11-10.30.7.254	10.10.100.140, 10.10.100.141
40	WLAN-Goscie	WLC-CPD - 10.40.0.2	10.40.0.11-10.40.7.254	10.10.100.140, 8.8.8.8
50	VLAN50-WIDI-AD	WLC-CPD - 10.50.0.2	10.50.0.11-10.50.0.254	10.10.100.140, 10.10.100.141
51	VLAN51-TABLETY	WLC-CPD - 10.50.1.2	10.50.1.11-10.50.1.254	10.10.100.140, 10.10.100.141
98	WLAN-AP-zarzadzanie	WLC-CPD - 10.10.98.1	10.10.98.2-10.10.98.254	brak
99	Zarzadzanie	SW-CPD-1 – 10.10.99.1	10.10.99.201-10.10.99.254	8.8.8.8

100	serwery	Brak	nd	nd
192	LAN-OLD	Przekierowanie do 10.10.100.140	b.d	10.10.100.140, 10.10.100.141
193	LAN_Tomografia	Brak	nd	nd
200	DMZ	brak	nd	nd
254	Polaczenie-LAN-UTM	brak	nd	nd

5.5 Zapobieganie pętlom w sieci – protokół STP

W celu zapobiegania powstaniu petli w sieci LAN pomiędzy portami switchy uruchomiono protokół STP (Spanning Tree Protocol) w trybie MSTP (MultiSpanning Tree Protocol), który zapewnia kontrolę pętli na poziomie VLANów.
Głównym punktem stosu STP dla każdego VLANu (ROOT) jest switch rdzeniowy SW-CPD-1 z ustawionym CIST BRIDGE = 0. Pozostałe switche mają wartość CIST Bridge domyślnie 32768. W razie awarii (niedostępności) switcha rdzeniowego, rolę ROOTa STP przejmie switch o najmniejszej (alfabetycznie) wartości adresu MAC.
Ponieważ protokół STP działa na zasadzie najmniejszego kosztu (najkrótszej drogi pakietów z uwględnieniem szybkości portów, topologia drzewa STP zmienia się automatycznie w zależności od aktywnych połączeń między switchami, a połączenie które, które fizycznie tworzą pętle w sieci wynikające z topologii fizycznej sieci, sa w stanie blokowania.
W normalnym stanie, gdy wszystkie połączenia fizyczne miedzy switchami są aktywne, w trybie blokowania sa linki oznaczone znaczkiem ⨯ na rysunku 1.

5.6 Routing w sieci

Switch rdzeniowy SW-CPD pracuje zapewnia routing między interfejsami warstwy 3-ej, tzn routing IP. Ruch do poszczególnych podsieci jest routowany zgodnie tablicą routingu.
Poniżej tablica routingu switcha.
Domyślnie ruch do innych podsieci niż te, dla których brama jest switch, jest kierowany na adres 10.10.254.254 czyli na adres firewalla/UTM Netasq, na którym jest już dalej skonfigurowany routing do internetu i do VLAN DMZ.

Konfiguracja domyślnego routingu:
ip route-static 0.0.0.0 0.0.0.0 10.10.254.254

Tablica routingu switcha:

```
[SW-CPD-1]dis ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 25        Routes : 25

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        0.0.0.0/0   Static  60   0           RD  10.10.254.254   Vlanif254
       10.10.99.0/24  Direct  0    0           D  10.10.99.1     Vlanif99
       10.10.99.1/32  Direct  0    0           D  127.0.0.1      Vlanif99
      10.10.100.0/24  Direct  0    0           D  10.10.100.1    Vlanif100
      10.10.100.1/32  Direct  0    0           D  127.0.0.1      Vlanif100
      10.10.254.0/24  Direct  0    0           D  10.10.254.1    Vlanif254
      10.10.254.1/32  Direct  0    0           D  127.0.0.1      Vlanif254
       10.20.0.0/21   Direct  0    0           D  10.20.0.1      Vlanif20
       10.20.0.1/32   Direct  0    0           D  127.0.0.1      Vlanif20
       10.30.0.0/21   Direct  0    0           D  10.30.0.1      Vlanif30
       10.30.0.1/32   Direct  0    0           D  127.0.0.1      Vlanif30
       10.40.0.0/21   Direct  0    0           D  10.40.0.1      Vlanif40
       10.40.0.1/32   Direct  0    0           D  127.0.0.1      Vlanif40
       10.50.0.0/24   Direct  0    0           D  10.50.0.1      Vlanif50
       10.50.0.1/32   Direct  0    0           D  127.0.0.1      Vlanif50
       10.50.1.0/24   Direct  0    0           D  10.50.1.1      Vlanif51
```

```
      10.50.1.1/32  Direct  0    0          D   127.0.0.1       Vlanif51
      10.50.2.0/24  Direct  0    0          D   10.50.2.1       Vlanif52
      10.50.2.1/32  Direct  0    0          D   127.0.0.1       Vlanif52
      127.0.0.0/8   Direct  0    0          D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0          D   127.0.0.1       InLoopBack0
    192.168.0.0/21  Direct  0    0          D   192.168.3.100   Vlanif192
  192.168.3.100/32  Direct  0    0          D   127.0.0.1       Vlanif192
  192.168.100.0/24  Direct  0    0          D   192.168.100.199 Vlanif193
192.168.100.199/32  Direct  0    0          D   127.0.0.1       Vlanif193

[SW-CPD-1]
```

5.7 Ograniczenie dostępu do innych podsieci – listy ACL

Ograniczenie diostepu do innych podsieci może być zrealizowane na:
- firewallu Netasq – ruch do internetu i DMZ oraz sieci wewnętrznych z internetu i DMZ
- switchu rdzeniowy WS-CPD – ruch między podsieciami wewnętrznymi (vlana-mi)
- kontrolerze WIFI – ruch z konkretnych sieci WLAN i klintów sieci

Na potrzeby ograniczenia dostępu miedzy sieciami wewnętrznymi zostały accesslisty na interfejsach switcha rdzeniowego oraz kontrolera WIFI.

a) ACL na switchu rdzeniowym

Na switchu rdzeniowym sa accesslisty przypisane statycznie do interfejsów, z których ma być ograniczony ruch.

Konfiguracja list ACL:

```
acl name do_Oracle 3000
 rule 5 permit tcp source 192.168.0.0 0.0.255.255 destination 10.10.100.100 0 destination-port eq 1521
 rule 10 permit icmp source 192.168.0.0 0.0.255.255 destination 10.10.100.100 0
 rule 20 permit tcp source 192.168.0.0 0.0.255.255 destination 10.10.100.100 0 destination-port eq 3389
 rule 55 permit icmp source 192.168.0.0 0.0.255.255
 rule 60 permit udp destination 10.10.100.100 0 destination-port eq ntp
 rule 65 permit udp destination 10.10.100.100 0 destination-port eq 563
 rule 90 deny ip destination 10.10.100.100 0
 rule 100 permit ip

acl name AMMS 3001
 rule 5 permit tcp source 10.50.2.0 0.0.0.255 destination 10.10.100.140 0 destination-port eq domain
 rule 10 permit udp source 10.50.2.0 0.0.0.255 destination 10.10.100.140 0 destination-port eq dns
 rule 15 permit tcp source 10.50.2.0 0.0.0.255 destination 10.10.100.141 0 destination-port eq domain
 rule 20 permit udp source 10.50.2.0 0.0.0.255 destination 10.10.100.141 0 destination-port eq dns
 rule 25 permit tcp source 10.50.2.0 0.0.0.255 destination 10.10.100.130 0 destination-port eq 8080
 rule 30 permit tcp source 10.50.2.0 0.0.0.255 destination 192.168.2.105 0 destination-port eq www
 rule 50 permit tcp source 10.50.2.0 0.0.0.255 destination 79.96.33.28 0 destination-port eq www
 rule 55 permit icmp destination 10.10.100.140 0
 rule 56 permit icmp destination 10.10.100.141 0
 rule 57 permit icmp destination 10.10.100.131 0
 rule 58 permit icmp destination 192.168.2.105 0
 rule 59 permit icmp destination 79.96.33.28 0
 rule 60 permit icmp destination 10.10.100.130 0
 rule 85 deny ip destination 192.168.0.0 0.0.255.255
 rule 90 deny ip destination 10.0.0.0 0.255.255.255
 rule 100 permit ip
```

przypisanie list do interfejsów:

```
traffic-filter vlan 192 inbound acl name do_Oracle
traffic-filter vlan 52 inbound acl name AMMS
```

b) ACL na kontrolerze WIFI

Na kontrolezre wifi sa skonfigurowane lsty ACL, które są dynamicznie przydzielane klientom WIFI przez reguły autoryzacyjne serwera AGILE dla sieci WLAN z autoryzacją radius

Konfiguracja list ACL:

```
acl number 3020     // accesslista przypisywana dynamicznie dla SSID WIFI_Pacjenci
 rule 5 permit tcp destination 10.10.100.140 0 destination-port eq domain
 rule 10 permit udp destination 10.10.100.140 0 destination-port eq dns
 rule 15 permit ip destination 10.10.100.10 0
 rule 20 deny ip destination 192.168.0.0 0.0.255.255
```

```
 rule 25 deny ip destination 10.0.0.0 0.255.255.255
 rule 30 permit ip

acl number 3030     // accesslista przypisywana dynamicznie dla SSID WIFI_Personel
 rule 5 permit tcp destination 10.10.100.141 0 destination-port eq domain
 rule 10 permit udp destination 10.10.100.141 0 destination-port eq dns
 rule 15 permit tcp destination 10.10.100.140 0 destination-port eq domain
 rule 20 permit udp destination 10.10.100.140 0 destination-port eq dns
 rule 25 permit ip destination 10.10.100.0 0.0.0.255
 rule 30 deny ip destination 10.0.0.0 0.255.255.255
 rule 35 permit ip destination 192.168.0.0 0.0.0.248
 rule 40 deny ip destination 192.168.0.0 0.0.255.255
 rule 50 permit ip

acl number 3040    // accesslista przypisywana dynamicznie dla SSID WIFI_Goscie
 rule 5 permit tcp destination 10.10.100.141 0 destination-port eq domain
 rule 10 permit udp destination 10.10.100.141 0 destination-port eq dns
 rule 15 permit tcp destination 10.10.100.140 0 destination-port eq domain
 rule 20 permit udp destination 10.10.100.140 0 destination-port eq dns
 rule 25 deny ip destination 10.0.0.0 0.255.255.255
 rule 30 deny ip destination 192.168.0.0 0.0.255.255
 rule 50 permit ip
#
```

6. Sieć bezprzewodowa

6.1 Opis budowy sieci WIFI

Siec WIFI został zbudowana zgodnie z projektem zamówienia, jako rozległa sieć WIFI z centralnym punktem zarządzania i serwerem autentykacji użytkowników Wifi, zapewniając różne metody autentykacji dla grup klientów WIFI, w tym autentykację użytkowników gościnnych z wykorzystaniem portalu autentykacji

Centralnym punktem sieci WIFI jest kontroler WIFI Huawei model AC6605 który kontroluje prace punktów dostępowych AP, przydziela dostępem klientów do poszczególnych sieci WLAN i zarządza ruchem sieciowym klientów WiFi do pozostałych segmentów sieci.

Autentykacja użytkowników do poszczególnych WLAN (SSID) odbywa się za pośrednictwem serwera autentykacji AGILE, który autentykuje klientów WIFI:

- poprzez portal autentykacji WEB dla gości i pacjentów szpitala oraz dla pracowników szpitala
- poprzez serwer domeny dla pracowników szpitala podsiadających konto w AD oraz urządzeń mobilnych szpitala (autentykacja metodą 802.1x)
- przez konta serwera Radius wbudowanego w serwer AGILE

Sieci WLAN (SSID) są dystrybuowane przez sieć LAN (przełączniki dystrybucyjne i dostępowe) do punktów dostępowych AP, do których łączą się bezprzewodowo klienci sieci WiFi.

Punkty dostępowe typu Huawei AP6010DN pracują w wersji LITE tylko pod kontrola Kontrolera WIFI i nie mogą pracować jako urządzenia samodzielne.

Punkty dostępowe zapewniają obsługę protokołów radiowych wg standaru 802.11 a,b,g,n,ac w dostępnych zakresach pasm częstotliwości 2,4Ghz i 5GHz

Komunikacja między kontrolerem WLC-CPD a AP-kami odbywa się protokołem CAPWAP , w dedykowanym VLAN98, który zapewnia komunikację kontrolną miedzy WLC a AP oraz tuneluje ruch klientów WIFI dla podsieci WLAN skonfigurowanych w trybie „tunel”.

Zarządzanie centralne punktami dostępowymi AP-kami przez WLC zapewnia :

- zapewnienie odpowiedniego poziomu mocy nadawania sygnału WIFI i kanał radiowy dla każdego AP – kontroler w czasie rzeczywistym dokonuje pomiarów interferencji sygnału między poszczególnymi AP-kami dopasowują nr kanału radiowego i moc nadawania radia
- bezprzerwowe przełączanie klientów WIFI między AP-kami w trakcie ruchu na terenie szpitala

obszarze objętym zasięgiem sygnału WIFI.

6.2 Wykaz urządzeń wchodzących w skład sieci WIFI

W poniższych tabelach zebrane zostały dane urządzeń Access Point zarządzanych przez kontrolerów WiFi WLC-CPD. W zestawieniu podano:

- typ punktu dostępowego (model)
- nazwa sieciowa , w której zaszyto lokalizację AP-ków wg klucza: Budynek_nr piętra_nr AP-ka, przy czym numerowanie APków na danym piętrze jest zgodne z ruchem wskazówek zegara od wejścia na korytarz oddziału
- numer seryjny
- nr ID na kontrolerze WLC
- adres fizyczny MAC na potrzeby lokalizacji w sieci na podstawie tablicy MAC switchy sieciowych

W zestawieniu zostały ujęte punkty dostępowe zainstalowane i podłączone do sieci zgodnie z projektem i wskazówkami inwestora. Nie zostały natomiast ujęte AP_ki dostarczone w ramach zamówienia, ale przeznaczone do montażu w późniejszym czasie przez inwestora

Tabela 8 Zestawienie punktów dostępowych AP sieci WiFi

TYP	Nazwa sieciowa	Numer seryjny	AP ID	adres MAC
AP6010DN-AGN	Bud_A_0P_1	2102354196W0EA001684	0	9017-acae-8760
AP6010DN-AGN	Bud_A_0P_2	2102354196W0EA001612	1	9017-acae-7e60
AP6010DN-AGN	Bud_A_0P_3	2102354196W0EA001647	2	9017-acae-82c0
AP6010DN-AGN	Bud_A_0P_4	2102354196W0EA001685	3	9017-acae-8780
AP6010DN-AGN	Bud_A_0P_5	2102354196W0EA001762	4	9017-acbe-54e0
AP6010DN-AGN	Bud_A_0P_6	2102354196W0EA001706	5	9017-acae-8a20
AP6010DN-AGN	Bud_A_1P_1	2102354196W0EA001610	6	9017-acae-7e20
AP6010DN-AGN	Bud_A_1P_2	2102354196W0EA001666	7	9017-acae-8520
AP6010DN-AGN	Bud_A_1P_3	2102354196W0EA001645	8	9017-acae-8280
AP6010DN-AGN	Bud_A_1P_4	2102354196W0EA001606	9	9017-acae-7da0
AP6010DN-AGN	Bud_A_2P_1	2102354196W0E8000781	10	1051-7228-80c0
AP6010DN-AGN	Bud_A_2P_2	2102354196W0E8000786	11	1051-7228-8160
AP6010DN-AGN	Bud_A_2P_3	2102354196W0E8000815	12	1051-7228-8500
AP6010DN-AGN	Bud_A_2P_4	2102354196W0E8000790	13	1051-7228-81e0
AP6010DN-AGN	Bud_A_2P_5	2102354196W0E8000788	14	1051-7228-81a0
AP6010DN-AGN	Bud_A_2P_6	2102354196W0E8000791	15	1051-7228-8200
AP6010DN-AGN	Bud_A_3P_1	2102354196W0EA001675	16	9017-acae-8640
AP6010DN-AGN	Bud_A_3P_2	2102354196W0EA001678	17	9017-acae-86a0
AP6010DN-AGN	Bud_A_3P_3	2102354196W0E8000784	18	1051-7228-8120
AP6010DN-AGN	Bud_A_3P_4	2102354196W0E8000795	19	1051-7228-8280
AP6010DN-AGN	Bud_A_3P_5	2102354196W0E8000789	20	1051-7228-81c0
AP6010DN-AGN	Bud_B_0P_1	2102354196W0E8000844	21	1051-7228-88a0
AP6010DN-AGN	Bud_B_0P_2	2102354196W0E8001035	22	1051-7228-a080
AP6010DN-AGN	Bud_B_0P_3	2102354196W0E8000787	23	1051-7228-8180
AP6010DN-AGN	Bud_B_0P_4	2102354196W0E8001034	24	1051-7228-a060
AP6010DN-AGN	Bud_B_0P_5	2102354196W0E8001029	25	1051-7228-9fc0
AP6010DN-AGN	Bud_B_1P_1	2102354196W0E8001007	26	1051-7228-9d00
AP6010DN-AGN	Bud_B_1P_2	2102354196W0E8001010	27	1051-7228-9d60

AP6010DN-AGN	Bud_B_1P_3	2102354196W0E8001008	28	1051-7228-9d20
AP6010DN-AGN	Bud_B_1P_4	2102354196W0E8001026	29	1051-7228-9f60
AP6010DN-AGN	Bud_B_2P_1	2102354196W0E8001011	30	1051-7228-9d80
AP6010DN-AGN	Bud_B_2P_2	2102354196W0E8001012	31	1051-7228-9da0
AP6010DN-AGN	Bud_B_2P_3	2102354196W0EA001769	32	9017-acbe-55c0
AP6010DN-AGN	Bud_B_2P_4	2102354196W0E8001014	33	1051-7228-9de0
AP6010DN-AGN	Bud_B_3P_1	2102354196W0EA001693	34	9017-acae-8880
AP6010DN-AGN	Bud_B_3P_2	2102354196W0E8000805	35	1051-7228-83c0
AP6010DN-AGN	Bud_B_3P_3	2102354196W0EA001609	36	9017-acae-7e00
AP6010DN-AGN	Bud_B_3P_4	2102354196W0EA001767	37	9017-acbe-5580
AP6010DN-AGN	Bud_B_4P_1	2102354196W0E8001027	38	1051-7228-9f80
AP6010DN-AGN	Bud_B_4P_2	2102354196W0E8001019	39	1051-7228-9e80
AP6010DN-AGN	Bud_B_4P_3	2102354196W0E8001033	40	1051-7228-a040
AP6010DN-AGN	Bud_B_4P_4	2102354196W0E8001031	41	1051-7228-a000
AP6010DN-AGN	Bud_B_5P_1	2102354196W0E8000783	42	1051-7228-8100
AP6010DN-AGN	Bud_B_5P_2	2102354196W0E8000785	43	1051-7228-8140
AP6010DN-AGN	Bud_B_5P_3	2102354196W0E8000782	44	1051-7228-80e0
AP6010DN-AGN	Bud_B_5P_4	2102354196W0E8000813	45	1051-7228-84c0
AP6010DN-AGN	Bud_B_5P_5	2102354196W0E8000799	46	1051-7228-8300
AP6010DN-AGN	Bud_B_6P_1	2102354196W0E8001044	47	1051-7228-a1a0
AP6010DN-AGN	Bud_B_6P_2	2102354196W0E8001001	48	1051-7228-9c40
AP6010DN-AGN	Bud_B_6P_3	2102354196W0E8000990	49	1051-7228-9ae0
AP6010DN-AGN	Bud_B_6P_4	2102354196W0EA001756	50	9017-acbe-5420
AP6010DN-AGN	Bud_B_6P_5	2102354196W0EA001738	51	9017-acae-8e20
AP6010DN-AGN	Bud_B_6P_6	2102354196W0E8001030	52	1051-7228-9fe0
AP6010DN-AGN	Bud_B_7P_1	2102354196W0E8001024	53	1051-7228-9f20
AP6010DN-AGN	Bud_B_7P_2	2102354196W0E8001020	54	1051-7228-9ea0
AP6010DN-AGN	Bud_B_7P_3	2102354196W0E8001038	55	1051-7228-a0e0
AP6010DN-AGN	Bud_B_7P_4	2102354196W0E8001039	56	1051-7228-a100
AP6010DN-AGN	Bud_B_8P_1	2102354196W0EA001743	57	9017-acae-8ec0
AP6010DN-AGN	Bud_B_8P_2	2102354196W0EA001723	58	9017-acae-8c40
AP6010DN-AGN	Bud_B_8P_3	2102354196W0EA001641	59	9017-acae-8200
AP6010DN-AGN	Bud_B_8P_4	2102354196W0EA001721	60	9017-acae-8c00
AP6010DN-AGN	Bud_B_8P_5	2102354196W0EA001749	61	9017-acae-8f80
AP6010DN-AGN	Bud_B_8P_6	2102354196W0EA001746	62	9017-acae-8f20

6.3 Wykaz sieci WLAN

W poniższej tabeli zawarte zostały sieci bezprzewodowe WLAN obsługiwane przez kontroler i AP-ki na terenie szpitala. Zestawienie zawiera :
- nazwa SSID – nazwa sieci WLAN ,
- rozgłaszanie – widoczność sieci WLAN w eterze
- vlan – przypisanie WLAn do podsieci VLAN

tryb rozgłaszania w eterze, nr vlanu przypisany do sieci, tryb transmisji danych,

Tabela 9 - Wykaz SSID

Nazwa SSID	Rozgłaszanie	vlan	Tryb transmisji	zabezpieczenie	Autentykacja / logowanie

WIFI_Pacjenci	Tak	20	Tunnel	Otwarta	Webportal / rejestracja + zatwierdzanie
WIFI_Personel	Tak	30	Tunnel	WPA-WPA2	Webportal / konta domenowe MSAD
WIFI_Goscie	Tak	40	Tunnel	otwarta	Webportal / rejestracja bez zatwierdzania
WIFI_AD_WSZS	Tak	50	Tunnel/Direct	DOT1x (802.11x)	Konta domenowe MSAD
TABLETY	Nie	51	Tunnel	DOT1x (802.11x)	Konta domenowe MSAD

6.4 Zarządzanie dostępem do sieci WIFI – autentykacja na serwerze Radius.

Dostęp do poszczególnych sieci WLAN jest zabezpieczony poprzez szyfrowanie i zabezpiecznie hasłem, z dodatkową autentykacją przez webportal lub otwarte tylko z autentykacją i autorejestracją przez webportal.
W powyższej tabeli nr 9 zawarto informacje o sposobie zabezpieczenia dostępu do sieci dla poszczególnych WLAN.
Dostęp do WLAN jest realizowany przez kontroler WiFi za pomocą autentykacji aaa przez serwer radiusa. Role serwera radius pełni serwer Agile – usługa uruchomiona na serwerze wirtualnym w środowisku VMWare o adresie 10.10.100.10.

6.4.1 Konfiguracja serwera Radius na kontrolerze WiFi

Ponizej konfiguracja serwera radius i autentykacji w poszczególnych vlanach i interfejsach ESS dla WiFi:
Klucze zabezpieczające komunikację z serwerem radius:

radius-server shared-key:	Agile_Bytom_key
radius-server authorization:	WLC_Charge_Key
shared-key	Web_Auth_key

```
radius-server template Agile
 radius-server shared-key cipher %@%@$>[SSB#uk<xg+|FE$t1#urT"%@%@
 radius-server authentication 10.10.100.10 1812 weight 80
 radius-server accounting 10.10.100.10 1813 weight 80
 undo radius-server user-name domain-included
radius-server authorization 10.10.100.10 shared-key cipher %@%@lzQw9WI*c%PN\p#x,nb&*yAU%@%@ server-group
Agile

aaa
 authentication-scheme default
 authentication-scheme Agile
  authentication-mode radius
authorization-scheme default
 authorization-scheme Agile
  authorization-mode if-authenticated local
 accounting-scheme default
 accounting-scheme Agile
  accounting-mode radius
  accounting realtime 15
 domain default
  authentication-scheme Agile
  accounting-scheme Agile
  authorization-scheme Agile
  radius-server Agile
#
url-template name portal
 url http://10.10.100.10:8080/portal
 url-parameter redirect-url url
```

```
#
web-auth-server Agile_portal
 server-ip 10.10.100.10
 port 50200
 shared-key cipher %@%@nM10JU9\D8aIg$K^jn91G]*z%@%@
 url-template portal
#
#
interface Vlanif20
 ip address 10.20.0.2 255.255.248.0
 web-auth-server Agile_portal direct
 dhcp select global
#
interface Vlanif30
 ip address 10.30.0.2 255.255.248.0
 web-auth-server Agile_portal direct
 dhcp select global
#
interface Vlanif40
 ip address 10.40.0.2 255.255.248.0
 web-auth-server Agile_portal direct
 dhcp select global
#
interface Vlanif50
 ip address 10.50.0.2 255.255.255.0
 web-auth-server Agile_portal direct
 portal domain default
 dhcp select global

interface Wlan-Ess50
 description ESS-AD
 port hybrid pvid vlan 50
 undo port hybrid vlan 1
 port hybrid untagged vlan 40 50
 dot1x enable
 dot1x authentication-method eap
 authentication restrict-vlan 40
 authentication guest-vlan 40
 permit-domain name default
 force-domain name default
#
interface Wlan-Ess51
 description ESS-TABLETY
 port hybrid pvid vlan 51
 undo port hybrid vlan 1
 port hybrid untagged vlan 51
 dot1x enable
 dot1x authentication-method eap
 permit-domain name default
 force-domain name default
 authentication max-user 30
```

7. Opis serwera Autentykacji AGILE

8. Czynności serwisowe

8.1 Zarzadzanie konfiguracją

Do urządzeń sieciowych można się zalogowac poprzez konsole ssh (zalecane) lub w trybie graficznym poprzez przeglądarkę internetową .
Do UPS-ów można się zalogować przez www lub telnet.
Do logowania po ssh i telnet można użyc dowolnego klienta ssh (np. putty) na standardowym porcie 2, a logowanie po http przez dowolną przeglądarkę www.
Lista adresów ip urządzeń znajduje się w tabeli nr 2
Dalsze przykłady konfiguracja przestawiono w oparciu o konsole terminalową (po ssh)
Alternatywnie można się do urządzeń logować przez dedykowany port konslowoy na urządzeniach – na te same konta administracyjne.
Logowanie odbywa się na konta lokalne urządzeń.

Po zalogowaniu użytkownik jest w trybie user mode:
<SW-CPD-1>

Przejście do trybu konfiguracji:
<SW-CPD-1>system-view
[SW-CPD-1]

Wyjście z trybu konfiguracji
[SW-CPD-1]return
<SW-CPD-1>

Założenie użytkownika lokalnego:

```
aaa                                                  //wejście w tryb lokalnego aaa
local-user administrator privilege level             // ustawienie poziomu dostępu
local-user administrator password haslo              // ustawienie hasła
local-user administrator service-type http ssh ftp   // typ dostępu
terminal                                             // Wyjście z aaa
quit                                                 // Konfiguracja ssh
ssh user administrator                               // Konfiguracja ssh - hasło
ssh user administrator authentication-type           // Konfiguracja ssh typ dostepu
password
ssh user administrator  service-type all
```

Komendy nawigacyjne:
Return // przejscie w tryb user
Quit // przejście poziom niżej w konfiguracji
Display this // konfiguracja w danej sekcji

8.2 Konfiguracja VLAN

Utworzenie – zarządzenie vlanem

```
display vlan                                         //wyświetlenie vlanów i portów do jakich sa
```

przypisane
vlan <nr x> // utworzenie vlanu nr x lub wejście w konfoguracje vlan
name nazwa // ustawienie nazwy vlan-u x

interface vlanx // przejście do interfejsu vlan x
desciption // opis interfejsu vlanx

Przypisanie vlan-u do vlanu nietagowane (w trybie access)

```
Interface GigabitEthernet 1/0/1     //wejście w tryb konfiguracji interfejsu np. Gi0/0/1
  port link-type access             // ustawienie interfejsu w trybie access
  port default-vlan x               // przypisanie vlan x do portu
```

Przypisanie vlanu tagowanego do portu w trybie trunk

```
Interface GigabitEthernet 1/0/2     //wejście w tryb konfiguracji interfejsu np. Gi0/0/1
  port link-type trunk              // ustawienie interfejsu w trybie trunk
  port trunk alloved-pass vlan x    // przypisanie vlan x do trunku (tagowane)
```

Interfejs VLAN warstwy 3 (IP)

Ustawienie Ip interfejsów powinno się nadawać tylko na przełaczniku rdzeniowym będącym bramą dla danej sieci (vlanu-u)

Nadanie adresu IP dla interfejsu

```
Interface vlan x                    //wejście w tryb konfiguracji interfejsu vlanx
  Ip address 1.2.3.4 24             // usatwienie dla interfesju vlan x adresu IP 1.2.3.4
                                    z maska 24bit (255.255.255.0)
  port trunk alloved-pass vlan x    // przypisanie vlan x do trunku (tagowane)
```

Konfiguracja DHCP dla vlanu - jako relay do innego serwera:

```
Interface vlan x                    //wejście w tryb konfiguracji interfejsu vlanx
   dhcp select relay                //właczenie trybu select
   dhcp relay server-ip 5.6.7.8     // skierowanie zapytań dhcp do serwera o IP 5.6.7.8
```

Konfiguracja DHCP na urzadzeniu

```
ip pool WIFI_pacjenci               //wejście w tryb konfiguracji puli dhcp
 gateway-list 10.20.0.1             // ustawienie Gateway
 network 10.20.0.0 mask 255.255.248.0   // ustawienie dla jakiej sieci IP ma być DHCP
 excluded-ip-address 10.20.0.2      // adresy IP które nie będą przypisywane
10.20.0.10                          // nadanie DNS dla sieci
 dns-list 10.10.100.140 8.8.8.8
```

8.3 Backup / odtwarzanie konfiguracji

Aby zgrać lub przywrócić konfiguracje musimy mieć podłączony do przełącznika na dowolnym VLAN komputer z serwerem TFTP.

Zapisanie konfiguracji (tylko w trybie user)

W trybie user <>

<SW-CPD-1>save

Backup konfiguracji na serwer tftp:

W trybie user <>

<SW-CPD-1>tftp serwer_IP put vrpcfg.zip nazwa.zip

Odtwarzanie konfiguracji z serwera tftp

W trybie user <>

<SW-CPD-1>tftp serwer_IP get nazwa.zip vrpcfg.zip

Restart urządzenia

9. Hasła

Wszystkie konta dostępowe i hasła, zarówno te do urządzeń sieciowych jak i te do sieci WIFI, zostaną przekazane w osobnym dokumencie.