

# ***Podręcznik Użytkownika do przełączników SRW224G4***



**Poznań 2010**

## 1. Informacje wstępne

Niniejszy podręcznik użytkownika opisuje specyfikację oraz podstawową konfigurację urządzeń Cisco SRW224G4.

### 2.1 Specyfikacja przełącznika



- 24 porty RJ-45 10/100 – Fast Ethernet,
- 4 porty RJ-45 10/100/1000 – Gigabit Ethernet,
- 2 gniazda mini-GBIC (współdzielone z portami GE),
- autonegocjacja duplexu i prędkości,
- samokrosujące się porty (Auto-MDI/MDIX),
- obsługa VLAN 802.11q (do 256 grup),
- tryby przyporządkowania portu do VLANu:
  - statyczny,
  - dynamiczny,
- obsługa ramek jumbo: mini jumbo (do 1600 bajtów),
- tablica adresów MAC 8kB,
- przepustowość wewnętrzna 12.8Gbps,
- QoS - przyporządkowywanie wag WRR (*Weight Round Robin*) / CoS (*Class of Service*) dla 4 kolejek na każdym porcie przełącznika,
- port mirroring - przekierowywanie ruchu z fizycznego portu na inny port,
- konfiguracja z poziomu przeglądarki WWW (http / https), telnet,
- spanning tree - IEEE 802.1d Spanning Tree, IEEE 802.1s Multiple Spanning Tree\*, IEEE 802.1w Rapid Spanning Tree\*, Fast Linkover\*,
- agregacja portów: do 8 portów w 8 grupach, obsługa LCAP,
- bezpieczeństwo: uwierzytelnianie użytkowników za pomocą protokołu 802.1x - Radius Authentication, MD5 Encryption,
- storm control: możliwość ograniczenia rozsyłania ramek broadcast / multicast / unknown unicast,
- testy okablowania miedzianego z poziomu przełącznika, ping, traceroute,
- możliwość aktualizacji firmware'u (TFTP, przeglądarka internetowa),
- zasilanie wewnętrzne,
- uchwyty do racka 19 cali,

wymiary: 430 x 44.45 x 202.5mm,

## 2.2 Konfiguracja przełącznika przez www

Wszystkie przełączniki zarządzalne firmy LINKSYS oferują użytkownikowi konfigurację urządzenia przy wykorzystaniu dwóch trybów:

- Konfiguracja z poziomu przeglądarki www, pozwala na zmianę praktycznie wszystkich parametrów i daje dostęp do zaawansowanych funkcji, szczegółowy opis w niniejszym rozdziale
- Konfiguracja przy użyciu portu konsoli, dostęp do podstawowych funkcji, tryb bardzo ważny przy aktualizacjach oprogramowania, odzyskiwaniu utraconych haseł, przywracania urządzenia do ustawień fabrycznych, szczegółowy opis tego trybu w rozdziale 2.3.

Może się zdarzyć, że nigdy nie użyjemy trybu dostępu do przełącznika przez port konsoli. Mimo to nie lekceważmy tego trybu, gdyż w pewnych sytuacjach może okazać się niedocenionym.

## 2.2.1 Konfiguracja podstawowa

Aby skonfigurować przełącznik przy użyciu przeglądarki www należy wpisać w polu adresu 192.168.1.254 (jest to domyślny adres konfiguracyjny switcha).



**UWAGA!** Komputer zarządzający musi mieć adres z podsieci, w której jest domyślny adres switcha czyli z podsieci 192.168.1.0, z maską 255.255.255.0. Jeżeli korzystamy z dynamicznego adresu, należy zmienić schemat adresacji na routerze (patrz rozdział 1.2.1). Jako rozwiązanie alternatywne należy przypisać do komputera statyczny adres IP. Zmiana domyślnego adresu możliwa jest dopiero po zalogowaniu na przełącznik lub przy użyciu konfiguracji przez port konsoli.

Po wpisaniu adresu i zatwierdzenia klawiszem Enter pojawi się ekran logowania:

Type in Username and Password, then click OK

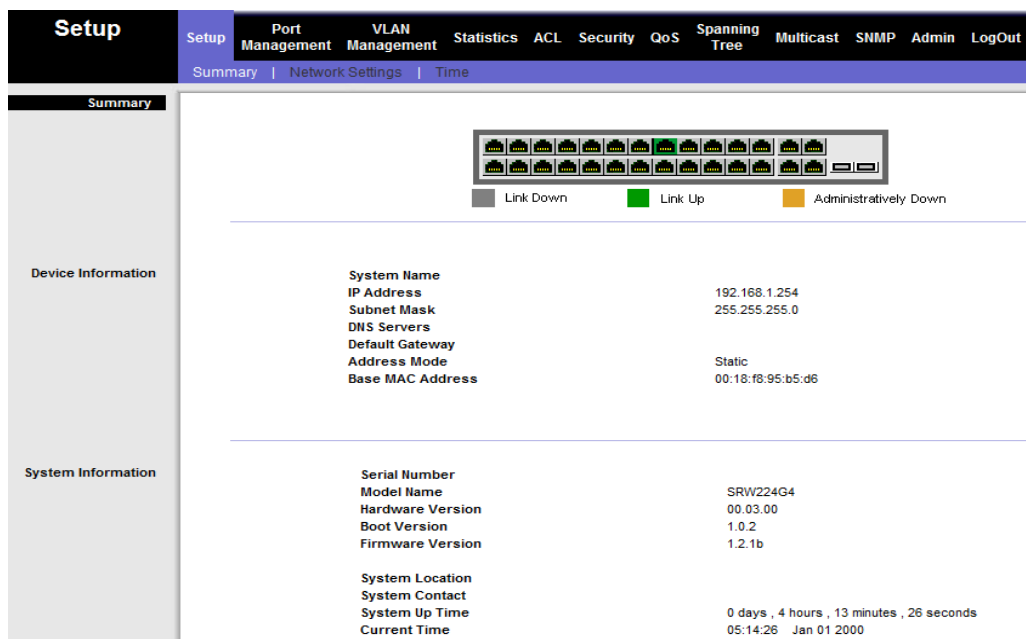
Username

Password

OK

W polach użytkownik (Username) i hasło (Password) należy wpisać admin (domyślna nazwa użytkownika i hasło do routera). Po kliknięciu OK, uzyskujemy dostęp do interfejsu zarządzania urządzeniem.

Zakładka Setup umożliwia monitorowanie podstawowych funkcji związanych z urządzeniem:



- Graficzna prezentacja stanu poszczególnych portów, port może znajdować się w jednym z 3 trybów:
  - Link Down – port nieaktywny, nic nie zostało do niego podłączone, lub nie ma łączności z podłączonym urządzeniem (np. urządzenie sieciowe ma odłączone zasilanie) – porty oznaczone na szaro
  - Link Up – port aktywny, do portu podłączono urządzenie, które jest aktywne, porty oznaczone na zielono
  - Administratively Down – administracyjnie wyłączony, na port nie jest podawane napięcie, nawet po podłączeniu aktywnego urządzenia port pozostanie nieaktywny – porty oznaczone na pomarańczowo
- Informacje dotyczące ustawień sieciowych:
  - Adres IP, maska, adres serwera DNS, bramy domyślnej
  - Tryb przypisania adresu, DHCP, Static IP
  - Adres MAC przełącznika
- Informacje dotyczące systemu:
  - Nazwa modelu
  - Wersja sprzętowa
  - Wersja pliku startowego
  - Wersja oprogramowania
- Informacje dodatkowe:
  - Nazwa systemu
  - Czas od włączenia urządzenia
  - Czas systemowy

W zakładce Network Settings istnieje możliwość nadania systemowi nazwy, określenie jego lokalizacji, a także kontaktu do administratora (opisywanie urządzeń ułatwia zarządzanie bardziej rozbudowanymi sieciami).

IP Configuration	
Management VLAN	1 ▾
IP Address Mode	DHCP ▾
Host Name	SRW24F4G
IP Address	192.168.3.60
Subnet Mask	255.255.255.0
Default Gateway	192.168.3.1
DNS Server	194.204.152.34

Dodatkowo użytkownik ma możliwość zmiany ustawień dotyczących adresu IP interfejsu zarządzającego. Tryby są analogiczne do trybów konfiguracji adresów IP w komputerze, przypisanie adresu przez DHCP (dynamiczne przypisanie adresu, switch staje się klientem serwera DHCP znajdującego się w naszej sieci, wybranie tego trybu wymaga od nas wiedzy jaki adres zostanie przypisany do switcha), lub statyczne przypisanie adresu (praktyka lepsza od przypisywania adresu przez DHCP, należy uważać, aby nie przypisać do urządzenia adresu, który jest już przypisany w naszej sieci do innego urządzenia).

Summary   Network Settings   Time	
<b>Network Settings</b>	
Identification	
System Name	<input type="text"/>
System Location	<input type="text"/>
System Contact	<input type="text"/>
System Object ID	1.3.6.1.4.1.3955.6.5024
Base Mac Address	00:18:f8:95:b5:d6

Podobnie jak w przypadku routera:

**UWAGA! Każda zmiana ustawień musi zostać zatwierdzona przez użytkownika poprzez kliknięcie przycisku zapisywania zmian -> Save Settings. Jeżeli wprowadziliśmy błędne dane możemy anulować zmiany poprzez kliknięcie -> Cancel Changes.**

Save Settings	Cancel Changes
---------------	----------------

Zakładka Time pozwala na konfigurację czasu. Użytkownik może ustalić czas systemowy statycznie, lub przy użyciu serwerów NTP. Więcej informacji na temat konfiguracji czasu systemowego w podręczniku obsługi użytkownika.

### 2.2.2 Zarządzanie portami

W zakładce Port Management, użytkownik ma możliwość zarządzania poszczególnymi portami przełącznika.

Port	Description	Administrative Status	Link Status	Speed	Duplex	MDI/MDIX	Flow Control	Type	LAG	PVE	Detail
e1		Up ▼	Up	100M	Full	MDIX	Disable	100M-copper			<a href="#">Detail</a>
e2		Up ▼	Down								<a href="#">Detail</a>
e3		Up ▼	Down								<a href="#">Detail</a>
e4		Up ▼	Down								<a href="#">Detail</a>

Powyższa tabelka prezentuje właściwości poszczególnych portów. Po kliknięciu przycisku Detail użytkownik może modyfikować poszczególne funkcje. Dokładny opis poszczególnych funkcji w rozdziale 2.2.2.1 Ustawienia podstawowe.

### 2.2.2.1 Ustawienia podstawowe

Funkcje modyfikowane przez użytkownika, dostępne po kliknięciu Detail:

- Opis portu(Description), dzięki opisywaniu portów, mamy możliwość określenia który z komputerów jest podłączony do którego portu switcha, dzięki temu łatwiej dotrzemy do komputera generującego szkodliwy ruch, lub zlokalizujemy uszkodzenie w naszej sieci
- Typ portu(Port Type) w tym wypadku port e1 to port 100Mb/s, miedziany(cooper),
- Status administracyjny(Admin Status) aktywny / nieaktywny - port odłączony administracyjnie),
- Status łącza(Current Port Status) jeżeli urządzenie podłączone do portu jest aktywne, port ma status Up,
- Wymuszenie określonej prędkości, trybu(half/full duplex) na porcie(Admin Advertisement)
- Auto-krosowanie portów(MDI/MDIX) w trybie auto, switch sam rozpozna jaki kabel jest podłączony i czy należy dokonać krosowania. Zastosowanie autokrosowania portów zdejmuje z użytkownika konieczność stosowania rodzaju okablowania odpowiedniego dla danego typu połączenia(możliwość stosowania zarówno kabli prostych, jak i krosowanych).

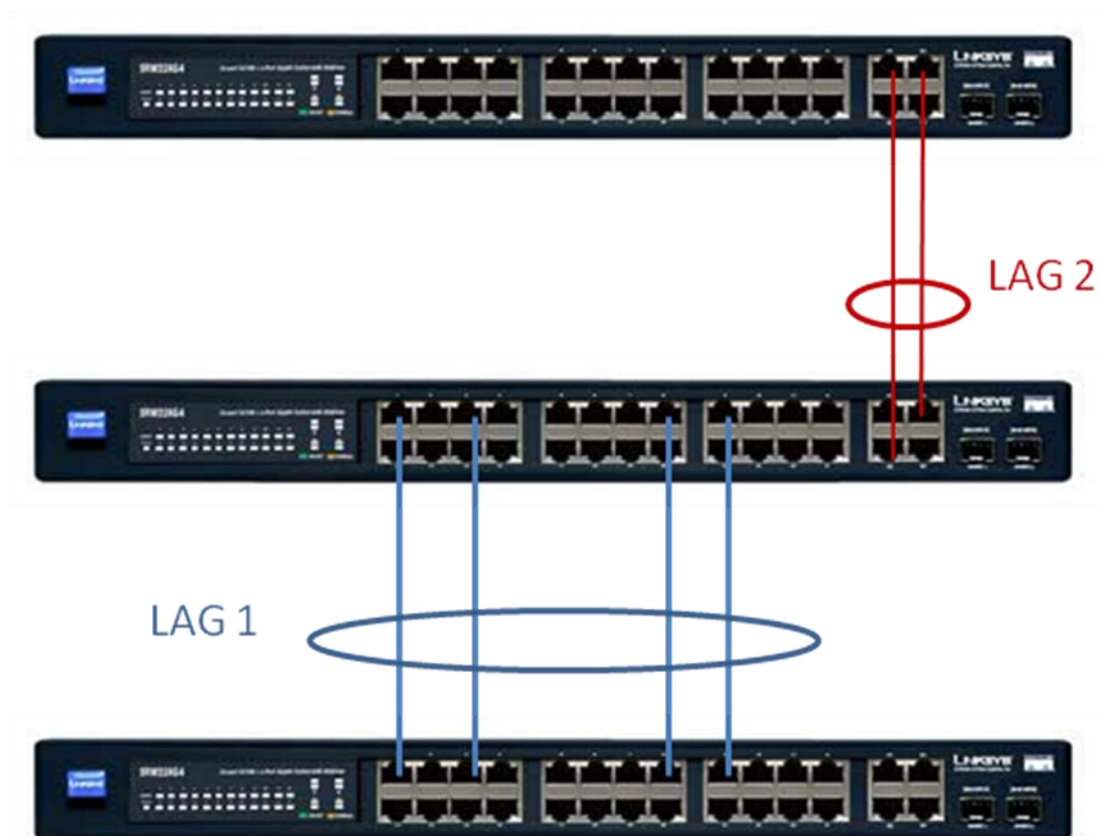


Port	e1 ▾
Description	<input type="text"/>
Port Type	100M-copper
Admin Status	Up ▾
Current Port Status	Up
Reactivate Suspended Port	<input type="checkbox"/>
Operational Status	Active
Admin Speed	100M ▾
Current Port Speed	100M
Admin Duplex	Full ▾
Current Duplex Mode	Full
Auto Negotiation	Enable ▾
Current Auto Negotiation	Enable
Admin Advertisement	<input checked="" type="checkbox"/> Max Capability <input type="checkbox"/> 10 Half <input type="checkbox"/> 10 Full <input type="checkbox"/> 100 Half <input type="checkbox"/> 100 Full
Current Advertisement	10 Half 10 Full 100 Half 100 Full
Neighbor Advertisement	10 Half 10 Full 100 Half 100 Full
Back Pressure	Disable ▾
Current Back Pressure	Disable
Flow Control	Disable ▾
Current Flow Control	Disable
MDI/MDIX	AUTO ▾
Current MDI/MDIX	MDIX
PVE	None ▾
LAG	

Pozostałe funkcje opisane w podręczniku obsługi użytkownika.

### 2.2.2.2 Agregacja łączy

Agregacja łączy ma na celu łączenie kilku interfejsów fizycznych przełącznika w jeden logiczny kanał. Użytkownik ma możliwość utworzenia do 8 grup łączy agregowanych, w każdym łączy agregowanym może się znajdować maksymalnie 8 portów fizycznych. Na poniższym rysunku zaprezentowano ideę tworzenia grup łączy agregowanych.



Z punktu widzenia switcha nie jest ważne gdzie znajdują się poszczególne interfejsy, ważne, aby wszystkie interfejsy włączone do grupy łączy agregowanych miały tę samą prędkość, tzn. w grupie łączy może się znajdować maksymalnie 8 portów FE lub 4 porty GE(ponieważ tyłoma dyspouje opisywany przełącznik). Na powyższym rysunku na switchu środkowym stworzono dwie grupy łączy agregowanych:

- LAG 1 – do tej grupy włączono 4 porty FastEth uzyskując łączną przepływność rzędu 800 Mb/s(ruch obustronny), w celu połączenia ze switchem dolnym
- LAG 2 – do tej grupy włączono 2 port GigabitEth, uzyskując łączną przepływność rzędu 4 Gb/s(ruch obustronny), w celu połączenia ze switchem górnym.

Tworzenie grup łączy agregowanych ma dwie główne zalety:

- Zwiększanie przepływności pomiędzy poszczególnymi segmentami sieci (np. pomiędzy dwoma switchami, maksymalna przepływność jaką można uzyskać agregując 4 porty typu Gigabit to 8 Gb/s biorąc pod uwagę ruch w obie strony).
- Nadmiarowość łączy, w przypadku uszkodzenia przewodu, lub awarii jednego z portów urządzenia są nadal połączone przez pozostałe porty należące do grupy łączy agregowanych.

Połączenie dwóch switchy przez kilka interfejsów nie przydzielonych do grupy łączy agregowanych, lub przez dwie grupy łączy agregowanych może skutkować w błędnym przesyłaniu pakietów. Switch nie będzie „wiedział” na który interfejs wysłać pakiet, ponieważ na każdym z nich będzie znalazł ten sam adres.

Aby stworzyć grupę łączy agregowanych należy:

- Przejść do zakładki Port Management->Link Aggregation
- Kliknąć Detail, przy wybranym numerze grupy łączy agregowanych(1-8)

LAG	Description	Admin Status	Type	Link Status	Speed	Duplex	Flow Control	LAG Mode	Detail
1		Up	Static		Unknown		Disable	Link Not Present	<a href="#">Detail</a>

- Pojawi się okno konfiguracji grupy łączy agregowanych

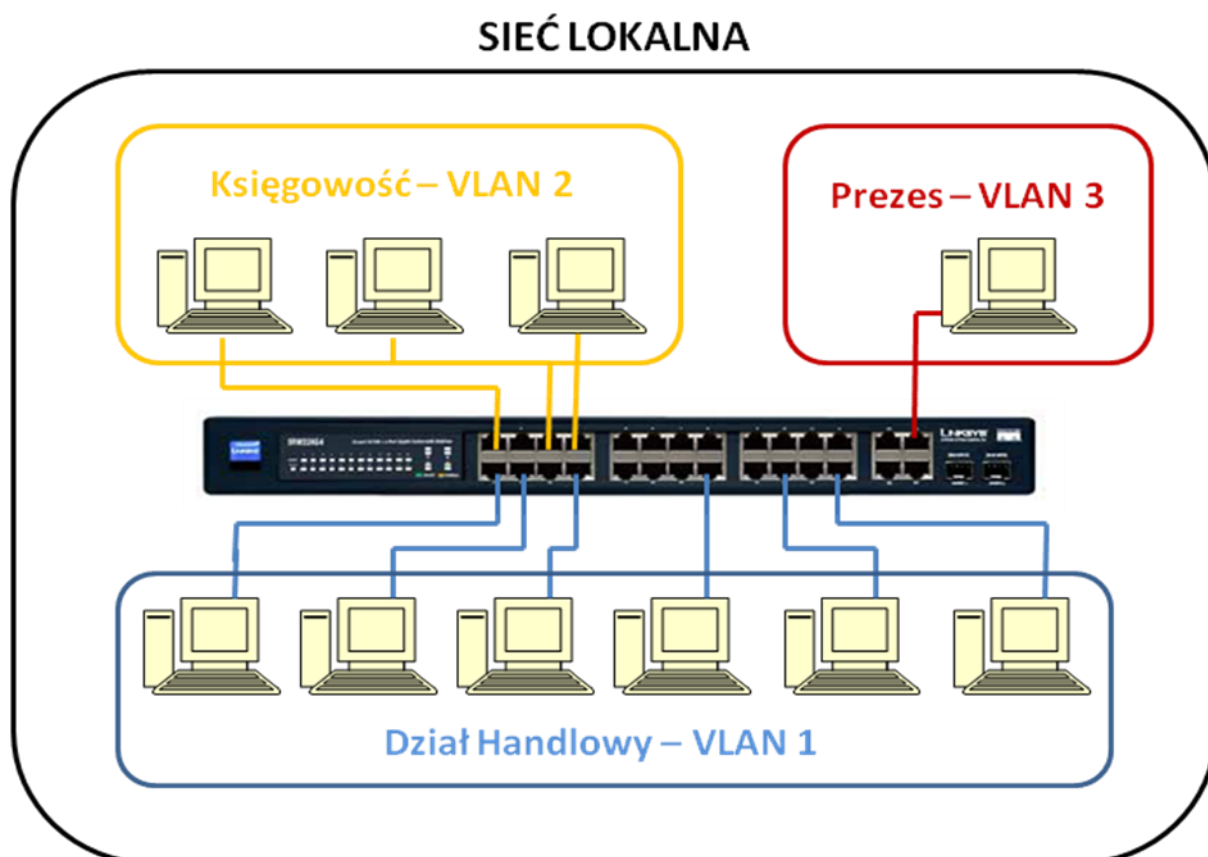
- Przypisać wybrane interfejsy do grupy łączy agregowanych(należy pamiętać, że do jednej grupy można przypisać tylko interfejsy o tej samej prędkości).

- Opcjonalnie można wprowadzić opis grupy łączy agregowanych (np. switch A - switch B).
- Dodatkowo użytkownik ma możliwość określenia statusu administracyjnego łącza (aktywne/nieaktywne).

Przykład zamieszczony na rysunku na poprzedniej stronie utworzył grupę łączy agregowanych o nazwie łącze A-B, status łącza został ustawiony na aktywny Up, a do grupy przypisano interfejsy e4, e5, e6, e7, zyskując łączną przepływność rzędu 400 Mb/s w jedną stronę.

### 2.2.3 Wirtualne sieci lokalne - VLAN

VLAN – czyli wirtualna sieć lokalna (Virtual Local Area Network) to najprościej mówiąc sieć w sieci. Przełączniki zarządzalne pozwalają nie tylko w łatwy sposób rozbudowywać istniejącą infrastrukturę, za ich pomocą możemy logicznie wydzielić poszczególne segmenty sieci tak aby ich użytkownicy się nie widzieli.



Dzięki takiej segmentacji, uzyskujemy 3 podsieci w obrębie jednej sieci lokalnej. Pomimo, że wszyscy użytkownicy podłączeni są do jednego switcha logicznie znajdują się w innych sieciach i nie „widzą” się nawzajem. W ten sposób użytkownicy

z działu handlowego nie mają dostępu do działu księgowości, czy komputera prezesa. Przenosząc powyższą sytuację na realia szkolnych pracowni internetowych, mamy możliwość rozdzielenia od siebie dwóch pracowni, komputera dyrektora lub sekretariatu pomimo wykorzystania do utworzenia infrastruktury jednego przełącznika.

Przełącznik daje nam możliwość utworzenia dwóch rodzajów VLANów:

- VLANy nietagowane – ten rodzaj wirtualnych sieci lokalnych, to rozdzielanie poszczególnych portów fizycznie na switchu, polega na przypisaniu konkretnych portów do wybranych wirtualnych sieci lokalnych.
- VLANy tagowane – dzięki VLANom tagowanym użytkownik ma możliwość rozpowszechniania informacji o istniejących na danym przełączniku wirtualnych sieciach lokalnych, każdy pakiet przypisany do VLANu tagowanego niesie ze sobą znacznik informujący urządzenia o jego przynależności do konkretnej podsieci. W celu współpracy pomiędzy urządzeniami sieciowymi świadomymi istnienia VLANów stworzono protokół 802.1q. Dzięki standaryzacji znaczników, możemy wykorzystać nasz przełącznik do łączności z innymi urządzeniami obsługującymi protokół 802.1q. Tagowanie ma jeszcze jedną istotną przewagę nad VLANami nie tagowanymi, pozwala na wykorzystanie do komunikacji między urządzeniami obsługującymi standard 802.1q łączy trunkingowych. Łącze typu trunk przenosi informacje pochodzące z VLANów do których należy. Przykładowym zastosowaniem łączy trunkingowych jest połączenie ze sobą dwóch switchy, pomimo, iż informacje między switchami będą wymieniane przy użyciu jednego łącza to każdy ze switchy będzie wiedział do której wirtualnej podsieci należy konkretny pakiet.

### 2.2.3.1 Tworzenie VLANów i łączy typu trunk

Tworzenie VLANów może wydawać się procesem skomplikowanym, jednak jak pokazano poniżej aby stworzyć VLAN i przypisać do niego konkretne porty wystarczy 3 proste kroki. W niniejszym przewodniku pokazano najprostszy sposób, w jaki można stworzyć VLANy tagowane.

#### KROK 1

Przejdź do zakładki VLAN Management -> Create VLAN

Create VLAN | Port Setting | Ports to VLAN | VLAN to Ports | GVRP

Create VLAN  
Single VLAN

VLAN ID (2-4094):

VLAN Name:

Update

W polu VLAN ID wpisujemy nr VLANu(zakres od 2-4094), VLAN nr 1 jest domyślnym VLANem, do którego należą wszystkie porty. Zarządzanie switchem możliwe jest tylko z portu należącego do VLANu 1 . Po wpisaniu nazwy możemy określić nazwę VLANu, na powyższym rysunku stworzono VLAN 3 o nazwie pracownia B. Po kliknięciu Update nowy VLAN trafi na listę istniejących sieci wirtualnych. Ostatnim elementem jest zapisanie zmian, czyli klikamy Save Settings. W polu VLAN Table znajdują się wszystkie utworzone VLANy wraz z nazwami i Statusem( domyślny - wbudowany w przełącznik VLAN zarządzający, statyczne – utworzone przez użytkownika na przełączniku, dynamiczne – rozpowszechnione przez protokół GVRP, nie opisywany w tym przewodniku).



VLAN ID	VLAN NAME	Status
1		Default
2	pracownia_A	Static
3	pracownia_B	Static

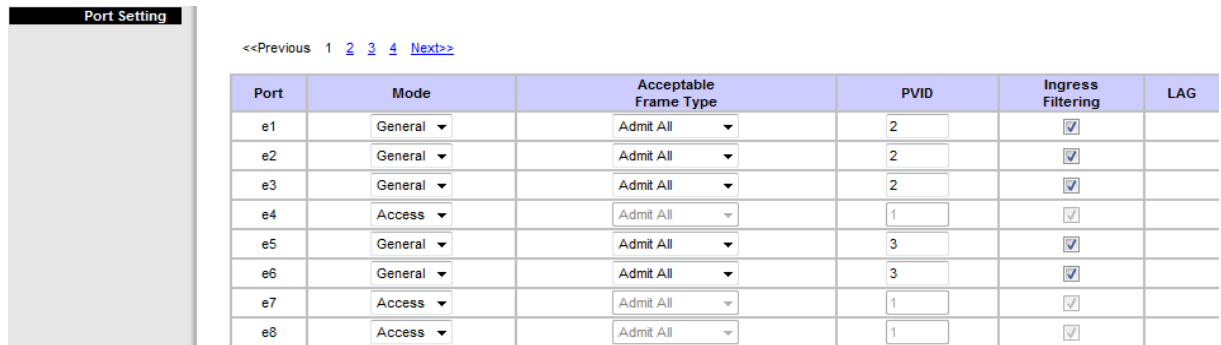
Jak można zaobserwować na powyższym rysunku oprócz VLANu domyślnego utworzono dwa VLANy statyczne o nr 2 – pracownia\_A, oraz o nr 3 – pracownia\_B.

### KROK 2

Zakładka VLAN Management -> Port Setting. W tej zakładce użytkownik definiuje w jakim trybie ma pracować dany port. W zależności od trybu pracy porty mogą być przypisywane do VLANów tagowanych, nietagowanych, lub występować jako łącza typu trunk pomiędzy dwoma switchami. Tryby pracy portów:

- Access, domyślnie wszystkie porty są w tym właśnie trybie, pozwala on na przypisanie poszczególnych portów tylko do 1 VLANu nietagowanego.
- General, ten tryb pozwala na przypisanie portu do VLANu zarówno nietagowanego jak i tagowanego, przy czym przy oznaczeniu VLANów jako nietagowanych, pakiety będą znacznikowane przy użyciu specjalnego pola określanego dla danego portu PVID. W przykładzie użyjemy właśnie trybu General oraz pola PVID, tak aby przynależność pakietu do konkretnego VLANu definiował nam statyczny znacznik.
- Trunk, tryb ten został omówiony na początku rozdziału, pozwala na przesyłanie informacji z VLANów tagowanych, pomiędzy urządzeniami obsługującymi protokół 802.1q.

W naszym przykładzie skorzystamy z dwóch utworzonych poprzednio VLANów, do VLANu 2 oznaczonego jako pracownia B, będziemy chcieli przypisać 3 porty FastEthernetowe, natomiast do VLANu 3 oznaczonego jako pracownia\_B przypiszemy 2 porty Fast Ethernetowe. Dodatkowo przyjmujemy, że jeden z portów gigabitowych będzie łączem typu trunk, aby wymieniać informację pomiędzy dwoma switchami.

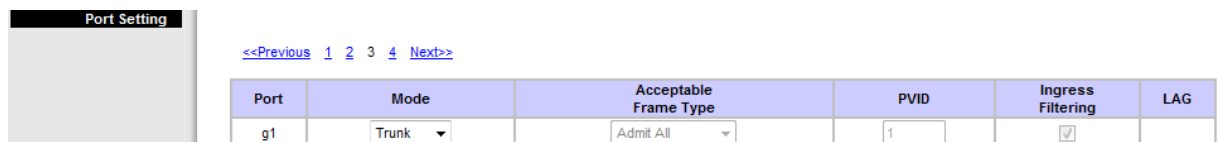


Port Setting

<<Previous 1 2 3 4 Next>>

Port	Mode	Acceptable Frame Type	PVID	Ingress Filtering	LAG
e1	General	Admit All	2	<input checked="" type="checkbox"/>	
e2	General	Admit All	2	<input checked="" type="checkbox"/>	
e3	General	Admit All	2	<input checked="" type="checkbox"/>	
e4	Access	Admit All	1	<input checked="" type="checkbox"/>	
e5	General	Admit All	3	<input checked="" type="checkbox"/>	
e6	General	Admit All	3	<input checked="" type="checkbox"/>	
e7	Access	Admit All	1	<input checked="" type="checkbox"/>	
e8	Access	Admit All	1	<input checked="" type="checkbox"/>	

Aby przypisać porty do VLANów zostały ustawione w tryb General. Ponadto określono PVID, zgodnie z nr do którego VLANu mają zostać przypisane. W ten sposób pakiet przychodzący na konkretnym porcie otrzyma indywidualny znacznik na podstawie PVID. Jak można zauważyć 5 portów ustawiono w tryb General, 3 z nich(e1, e2, e3) przypisano PVID=2 (zostaną przypisane do VLANu 2), 2 z nich(e5, e6) przypisano PVID=3(zostaną przypisane do VLANu 3). Dodatkowo jak na poniższym rysunku port g1 został ustawiony w tryb Trunk.



Port Setting

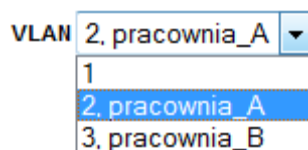
<<Previous 1 2 3 4 Next>>

Port	Mode	Acceptable Frame Type	PVID	Ingress Filtering	LAG
g1	Trunk	Admit All	1	<input checked="" type="checkbox"/>	

Po zapisaniu ustawień mamy 2 kroki w tworzeniu VLANów za sobą.

### KROK 3

Ostatnim elementem w tworzeniu wirtualnych sieci lokalnych, jest przypisanie portu do konkretnego VLANu. Aby przypisać port do VLANu należy przejść do zakładki VLAN Management -> Ports to VLAN. Z listy rozwijalnej należy wybrać nr VLANu, do którego chemy przypisać dany port, czyli najpierw VLAN 2:



Po wybraniu konkretnego VLANu zaznaczamy, które z portów mają być w tym VLANie.

VLAN 2, pracownia\_A

Eth	e1	e2	e3	e4	e5	e6	e7	e8	e9	e10	e11	e12	e13	e14	e15	e16	e17	e18	e19	e20	e21	e22	e23	e24
Access	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Trunk	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
General	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Tagged	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
UnTagged	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Forbidden	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Exclude	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Porty e1, e2, e3 zostały przypisane do VLANu 2 jako nietagowane. Nietagowane, ponieważ pakiety wchodzące na port nie posiadają znaczników. Znacznik jest przypisywany do VLANu dopiero w porcie, przez wcześniej określony parametr PVID. Po przejściu przez port pakiet staje się tagowanym.

Analogicznie przypisujemy porty e5 oraz e6 do VLANu nr 3 – pracownia\_B:

VLAN 3, pracownia\_B

Eth	e1	e2	e3	e4	e5	e6	e7	e8	e9	e10	e11	e12	e13	e14	e15	e16	e17	e18	e19	e20	e21	e22	e23	e24
Access	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Trunk	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
General	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Tagged	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
UnTagged	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Forbidden	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Exclude	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

W ten sposób zakończyliśmy tworzenie VLANów. Pozostaje nam tylko przypisanie portu Trunk do VLANów, z których informacje nasze łącze trunkingowe ma przesyłać. W naszym wypadku jako łącze trunkingowe przypisaliśmy g1, więc musimy je dodać zarówno do VLANu 2 oraz 3.

Gigabit	g1	g2	g3	g4
Access	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Trunk	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
General	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Tagged	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
UnTagged	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Forbidden	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Exclude	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

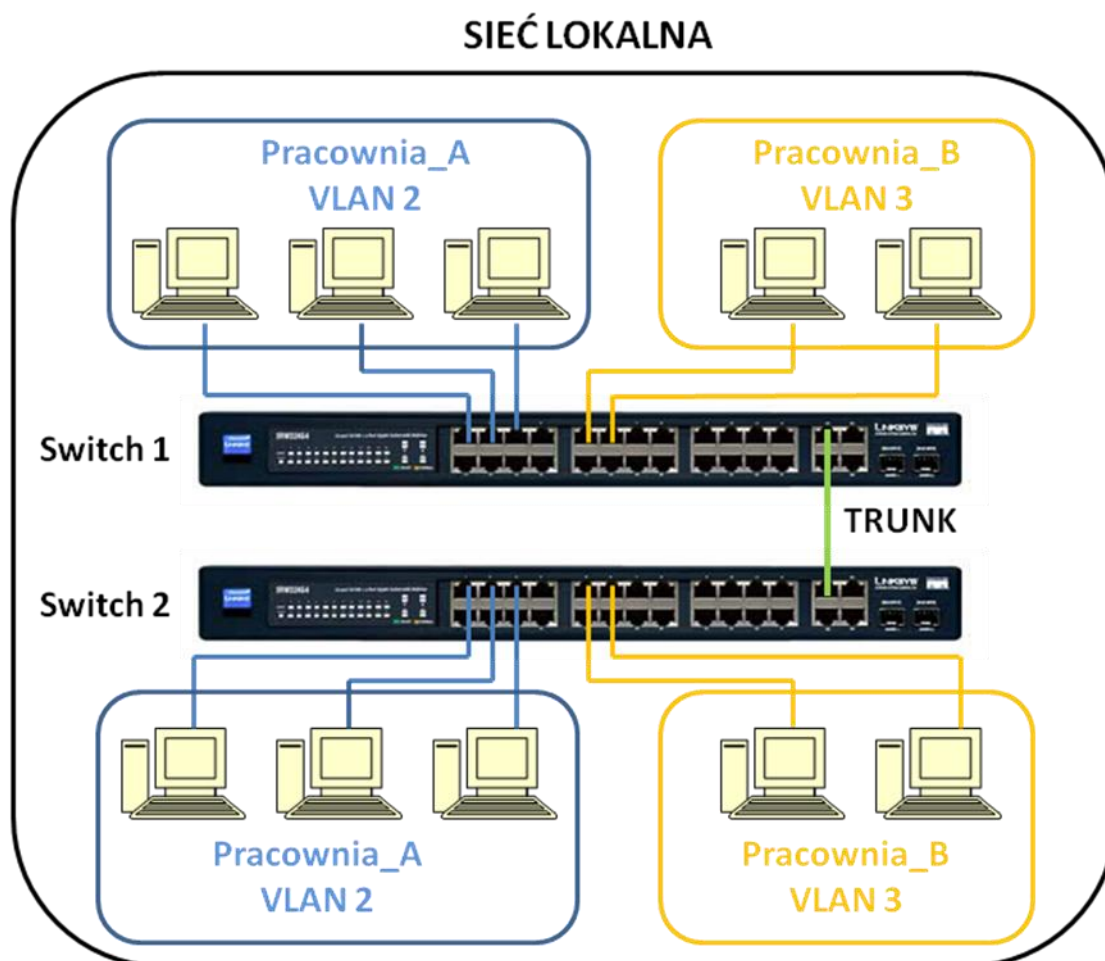
W dokładnie ten sam sposób w który przypisaliśmy poprzednie porty do VLANów przypisujemy łącze g1. W tym momencie użytkownik ma do wyboru jedynie tryb



tagowany, ponieważ pakiety które przeszły przez porty należące do któregoś z VLANów są tagowane znacznikiem wpisanym przez nas w polu PVID.

Zakończyliśmy tworzenie wirtualnych sieci lokalnych na naszym switchu. Jeżeli powyższe kroki zostały przeprowadzone zgodnie z przedstawioną procedurą uzyskaliśmy 3 sieci wirtualne w obrębie jednego switcha (pamiętajmy, że porty nie przypisane do żadnego z VLANów ciągle należą do VLANu domyślnego czyli VLANu o nr 1).

Aby ułatwić zrozumienie uzyskanego efektu przedstawiono je na przykładzie zestawienia takiej samej konfiguracji na dwóch switchach SRW224G4 połączonych ze sobą łączem typu trunk. Jak pokazano w dalszej części tego przewodnika, wystarczy skonfigurowanie jednego urządzenia, a następnie eksport pliku konfiguracyjnego na lokalnie podłączony komputer (Roz. 2.2.10.5), w kolejnym kroku stworzoną konfigurację importujemy do drugiego urządzenia, uzyskując dwa przełączniki o tej samej konfiguracji.



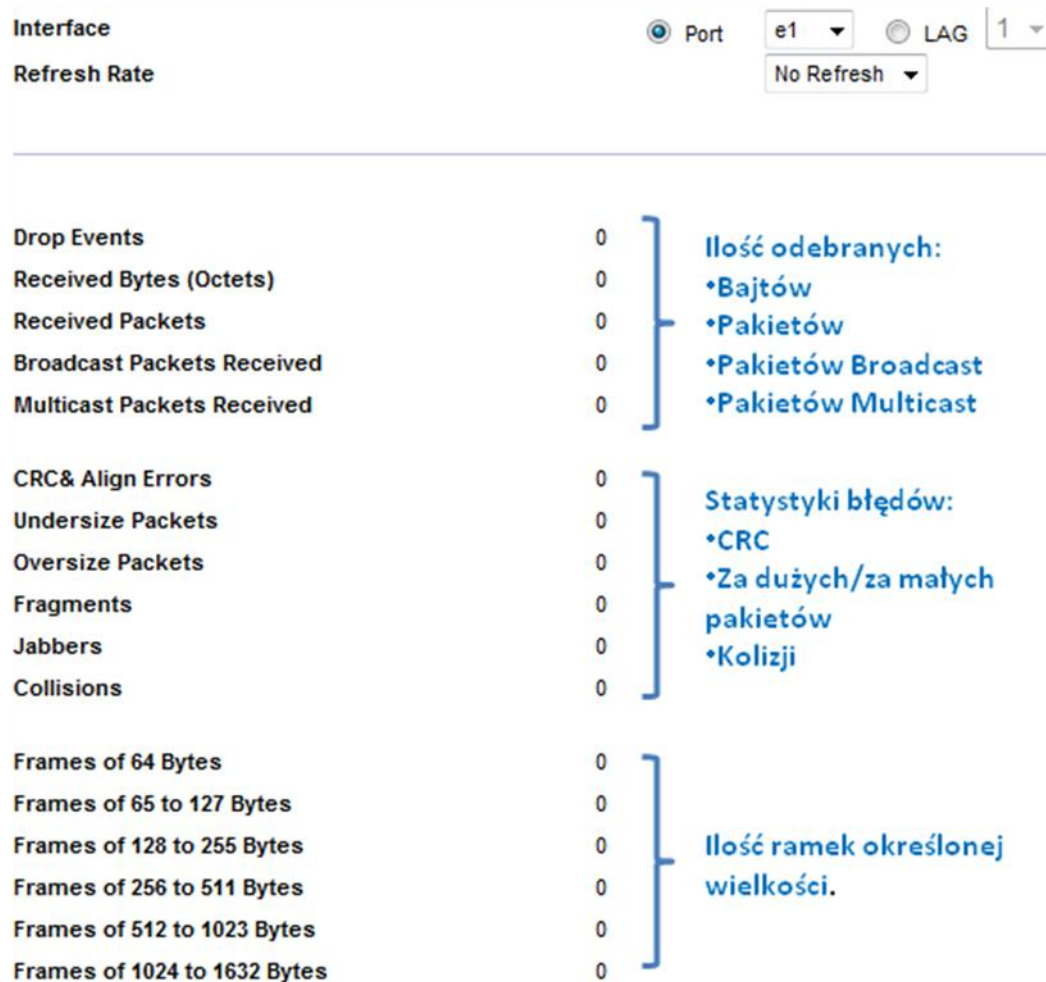
Na powyższym rysunku przedstawiono efekt skonfigurowanych przez nas VLANów. Co uzyskujemy dzięki takiej konfiguracji:

- Komputery widzą się wzajemnie w ramach jednego VLANu (niezależnie od tego do którego switcha zostały podłączone, łącze typu TRUNK oznaczone kolorem zielonym przenosi ruch należący do VLANów 2 i 3 pomiędzy switchami).
- Komputery nie widzą się wzajemnie jeżeli znajdują się w jednym VLANie, komputery z pracowni\_B nie widzą komputerów z pracowni\_A (zarówno w obrębie jednego przełącznika, jak i na oddzielnych przełącznikach).

### 2.2.4 Statystyki

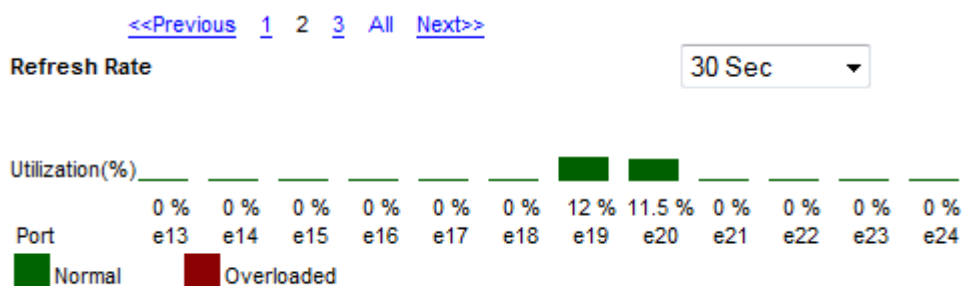
W zakładce Statistics użytkownik ma możliwość monitorowania zarówno podstawowych parametrów związanych z transmisją, jak przepływność na poszczególnych portach, aż po śledzenie błędnych ramek i uszkodzonych pakietów. Dzięki właściwemu wykorzystaniu funkcji pozwalających śledzić statystyki możemy zarządzać naszą siecią mądrzej i uczynić ją bardziej wydajną.

Zakładka Statistics-> RMON Statistics pozwala na śledzenie szczegółowych statystyk dla poszczególnych interfejsów.



Oprócz śledzenia statystyk na poszczególnych portach, użytkownik, ma możliwość ustalania zdarzeń, a co za tym idzie generowania przy ich pomocy alarmów systemowych, w zależności od wybranego typu. Do ustawiania zdarzeń i alarmów systemowych, służą kolejne podzakładki, znajdujące się w głównej zakładce Statistics. Dokładniejszy opis poszczególnych z nich w podręczniku obsługi użytkownika.

Graficzna reprezentacja wykorzystania poszczególnych z portów jest dostępna w zakładce Statistics->Port Utilization.



Użytkownik ma możliwość wyboru szybkości odświeżania (15, 30 lub 60 sekund) i graficznego śledzenia wykorzystania poszczególnych portów. Na rysunku na poprzedniej stronie można zauważyć, że porty e19 i e20 były wykorzystywane w danym momencie. Zasadniczo, jeżeli nie generujemy większego ruchu, nie przesyłamy plików przez któryś z interfejsów na switchu, wykorzystanie portów będzie się utrzymywać na poziomie 0 %. Jeżeli dany z portów będzie przeciążony, generowany ruch będzie większy niż możliwości transferu na porcie, zostanie on oznaczony na czerwono jako Overloaded.

Poza statystykami związanymi ściśle z wykorzystaniem poszczególnych interfejsów switcha, użytkownik może sprawdzić statystyki związane z protokołem 802.1x (zakładka Statistics->802.1x Statistics), a także protokołem dynamicznego rozpowszechniania VLANów GVRP (zakładka Statistics->GVRP Statistics).

### 2.2.5 Listy dostępu

Listy dostępu to narzędzie administracyjne pozwalające określić administratorowi sieci dostęp poszczególnych użytkowników do określonych usług sieciowych. Listy dostępu przypominają funkcjonalnością polityki dostępu, opisane dokładniej w rozdziale 1.2.4. Na różnicę pomiędzy politykami dostępu i listami dostępu składa się kilka elementów:

- Brak możliwości określenia czasu obowiązywania listy dostępu;
- Brak możliwości blokowania nazw domenowych, lub słów kluczowych w listach dostępu;
- Możliwość powiązania listy dostępu z określonym portem fizycznym, lub grupą łączy agregowanych przełącznika;
- Możliwość określenia nie tylko adresu źródłowego, ale i adresów docelowych dla których ma obowiązywać dana lista, czyli blokowanie ruchu już w obrębie danego segmentu sieci kontrolowanego przez switch;
- Możliwość określenia czynności która ma zostać wykonana w przypadku złamania polityki dostępu:
  - Pozwolenie na ruch

- Zablokowanie ruchu
- Zablokowanie ruchu i administracyjne wyłączenie portu(od tej chwili port będzie administracyjnie wyłączony, aż do czasu ponownego odblokowania przez administratora).

### 2.2.5.1 Tworzenie list dostępu

Aby utworzyć listę dostępu należy przejść do zakładki ACL. Kolejnym krokiem jest wybór typu listy dostępu z jakiej mamy korzystać. Użytkownik ma możliwość wyboru dwóch rodzajów list dostępu:

- **IP** – bardziej zaawansowana, pozwala na blokowanie konkretnych serwisów sieciowych po numerach portu, określono następujące rodzaje ruchu TCP/UDP/IGMP/ICMP/OSPF/EIGRP, dodatkowo użytkownik ma możliwość blokowania ruchu po określonych przez siebie portach
- **MAC** – mniej zaawansowane pozwalają na blokowanie całego ruchu z danych adresów MAC na inne adresy MAC

Ponieważ tworzenie list dostępu IP daje użytkownikowi więcej funkcjonalności i jest bardziej elastyczne dlatego na tym typie list skupiono się w dalszej części tego przewodnika.

W celu utworzenia listy dostępu IP należy przejść do zakładki ACL->IP Based ACL. Kolejno należy określić:

- Nazwę polityki dostępu

The screenshot shows two radio buttons. The first is labeled 'ACL Name' and is selected, with a dropdown menu showing 'Select an ACL'. Below it is a 'Delete ACL' link. The second radio button is labeled 'New ACL Name' and is not selected, with a text input field containing 'lista2'.

- Rodzaj akcji jaka ma zostać wykona w przypadku złamania reguły polityki dostępu: Permit(dopuszcz ruch), Deny(zablokuj ruch), Shutdown(zablokuj ruch i administracyjnie wyłącz port)
- Protokół transportowy który ma zostać zablokowany: z listy rozwijalnej, dla określonego nr portu, lub dla transmisji z określonego portu źródłowego do portu docelowego(tylko dla protokołów TCP/UDP). Dodatkowo użytkownik ma możliwość decyzji(dla protokołu TCP) jakie flagi w pakiecie mają być brane pod uwagę przy filtrowaniu
- Adres źródłowy/adres docelowy, przy określaniu adresu docelowego oraz adresu źródłowego, użytkownik ma możliwość określenia grupy adresów, przy użyciu parametru Wild Card Mask. Zadaniem parametru Wild card Mask jest maskowanie adresu IP. Aby polityka dotyczyła konkretnego adresu IP maska musi zostać ustawiona na 0.0.0.0, aby dotyczyła dowolnego adresu IP maska musi zostać ustawiona na 255.255.255.255.

Przyjmijmy, że chcemy aby polityka dotyczyła wszystkich adresów z podsieci 192.168.1.0/24. Jako adres IP wpisujemy 192.168.1.0 a jako maskę 0.0.0.255

Aby zrozumieć dokładniej funkcje maskowania adresu należy zastosować zapis binarny.

192.168.1.0 : 11000000.10101000.00000001.00000000  
0.0.0.255 : 00000000.00000000.00000000.11111111

Powyższy zapis oznacza, że polityka będzie dotyczyła adresów z zakresu 192.168.1.1 – 192.168.1.255.

Miejsca w których w Wild Card Mask występują jedynki nie są porównywane ze wzorcem adresu, powoduje to że w ostatnim oktecie może wystąpić dowolna wartość. Miejsca w których występuje 0 oznaczają że ta część adresu IP musi się dokładnie zgadzać z podanym wzorcem.

The screenshot shows a configuration form for a network rule. The 'Action' is set to 'Shutdown'. Under 'Protocol', 'Select from List' is chosen with 'UDP' selected, and 'Protocol ID To Match' is set to '17'. The 'TCP Flags' section includes 'Urg', 'Ack', 'Psh', 'Rst', 'Syn', and 'Fin', each with a 'Set' dropdown menu. 'Source Port' and 'Destination Port' are both set to 'Any'. 'Source IP Address' is '192.168.3.44' and 'Destination IP Address' is '192.168.3.1', both with 'Wild Card Mask' set to '0.0.0.0'. 'Match DSCP' is checked, and 'Match IP Precedence' is unchecked. An 'Add to List' button is located at the bottom of the form.

- Ostatni element odnosi się do usługi związanej z zapewnianiem właściwego priorytetu ruchu na podstawie wartości pola w pakiecie określanego jako DSCP, wykorzystanie tego pola wymaga przypisywania pakietów do właściwych klas ruchowych w sieciach z zaimplementowaną architekturą DiffServ.

W ten sposób stworzona została lista dostępu, śledząc powyższe dane można zauważyć, że polityka blokuje ruch po protokole UDP, z adresu 192.168.3.44 na adres 192.168.3.1. Ostatnim elementem związanym z tworzeniem listy dostępu jest przypisanie jej do konkretnego interfejsu fizycznego na przełączniku, któremu poświęcony jest kolejny rozdział.

Po dodaniu określonej utworzonej listy do tabeli list istniejących poprzez kliknięcie Add to List i zapisanie ustawień mamy pierwszy krok w tworzeniu list dostępu za sobą.

Przyjmując, że dana lista została już przypisana do interfejsu, do którego podłączono hosta o adresie 192.168.3.44, poniżej zaprezentowano wartości uzyskane w wyniku testowania łączności pomiędzy adresami 192.168.3.44, a 192.168.3.1. Test został przeprowadzony przy użyciu podstawowego narzędzia wbudowanego w system Windows, wysyłania wiadomości ping. Strona lewa prezentuje test przed utworzeniem listy, a strona prawa po utworzeniu listy dostępu.

```
C:\>ping 192.168.3.1
Badanie 192.168.3.1 z 32 bajtami danych:
Odpowiedź z 192.168.3.1: bajtów=32 czas=1ms TTL=255
Odpowiedź z 192.168.3.1: bajtów=32 czas=1ms TTL=255
Odpowiedź z 192.168.3.1: bajtów=32 czas<1 ms TTL=255
Odpowiedź z 192.168.3.1: bajtów=32 czas=1ms TTL=255
Statystyka badania ping dla 192.168.3.1:
Pakiety: Wysłane = 4, Odebrane = 4, Utracone = 0 (0% straty),
Szacunkowy czas błędzenia pakietów w milisekundach:
Minimum = 0 ms, Maksimum = 1 ms, Czas średni = 0 ms

C:\>ping 192.168.3.1
Badanie 192.168.3.1 z 32 bajtami danych:
Upłynął limit czasu żądania.
Upłynął limit czasu żądania.
Upłynął limit czasu żądania.
Upłynął limit czasu żądania.
Statystyka badania ping dla 192.168.3.1:
Pakiety: Wysłane = 4, Odebrane = 0, Utracone = 4 (100% straty),
```

### 2.2.5.2 Powiązanie listy dostępu z portem przełącznika

Aby lista dostępu działała, nie wystarczy jej utworzenie, drugim krokiem w procesie tworzenia list jest ich przypisywanie do określonych portów na przełączniku. Aby przypisać określoną listę dostępu do danego portu przełącznika należy przejść do zakładki Security -> ACL Binding

Interface	<input checked="" type="radio"/> Port	e1	<input type="radio"/> LAG	1
ACL Name	<input checked="" type="radio"/> IP Based ACL	lista1	<input type="radio"/> MAC Based ACL	

Listę dostępu przypisujemy do konkretnego interfejsu, lub grupy łączy agregowanych. Po wybraniu interfejsu decydujemy do jakiego typu Access listy ma zostać przypisany interfejs: IP/MAC. Następnie decydujemy, do której listy przypisać dany interfejs. Interfejs może zostać przypisany jednocześnie do kilku list dostępu. Po kliknięciu Add to List i zapisaniu ustawień, w tabeli pojawia się lista, do których list dostępu przypisane zostały poszczególne interfejsy.



### 2.2.6 Funkcje bezpieczeństwa

Przełącznik oferuje użytkownikowi szeroki zakres funkcji bezpieczeństwa. W zależności od zastosowanego sprzętu sieciowego dysponujemy bardziej, lub mniej zaawansowanymi funkcjami bezpieczeństwa.

Zaawansowane funkcje bezpieczeństwa opierają się na wykorzystaniu protokołów bezpieczeństwa i serwerów uwierzytelniających. Po podłączeniu do przełącznika systemu pracującego jako serwer RADIUS, lub TACACS uzyskujemy scentralizowaną bazę autoryzacji klientów naszego przełącznika. Dane wszystkich hostów zapisane są w jednym miejscu, autoryzacja może odbywać się na podstawie sprawdzenia nazwy użytkownika, hasła, lub chociażby adresu MAC poszczególnych urządzeń. Po podłączeniu użytkownika do przełącznika, urządzenie skontaktuje się z serwerem czy taki użytkownik istnieje i czy ma prawo dostępu do naszej sieci. Oprócz typowych serwerów RADIUS istnieje możliwość autentykacji typu host/MAC based przy wykorzystaniu protokołu 802.1x.

Podstawowe funkcje bezpieczeństwa, nie wymagają podłączania do przełącznika zewnętrznych serwerów uwierzytelniających, dlatego w niniejszym podręczniku skupimy się na funkcjach dostępnych przy użyciu funkcji wbudowanych w przełącznik.

#### 2.2.6.1 Autentykacja na podstawie adresu MAC

Przełącznik daje administratorowi możliwość autentykacji użytkowników na podstawie adresów MAC poszczególnych urządzeń. Ten rodzaj uwierzytelniania pozwala na zapisanie w konfiguracji przełącznika, który host podłączony jest do którego portu na naszym przełączniku. Switch oferuje dwa tryby przypisywania adresów MAC do poszczególnych portów:

- Zamek klasyczny(Classic Lock) – pozwala na przypisanie pojedynczego adresu MAC do interfejsu fizycznego przełącznika
- Zamek dynamiczny(Dynamic Lock) – administrator ma możliwość określenia, ilu użytkowników może zostać poznanych na danym porcie, funkcję tą wykorzystujemy, gdy do danego portu na przełączniku podłączają się różni użytkownicy, lub gdy dany port wykorzystywany jest do rozszerzania naszej sieci o kolejne elementy( np. o kolejny przełącznik)

W momencie zamknięcia danego interfejsu, pojawienie się na nim nieznanego adresu MAC spowoduje akcję zaplanowaną na takie zdarzenie, administrator ma do wyboru 3 rodzaje czynności, jakie mogą zostać w tym wypadku wykonane:

- Normalne przekazywanie ruchu(Forward Normal)
- Blokowanie ruchu pochodzącego od nieznanego hosta(Discard)
- Blokowanie ruchu oraz administracyjne wyłączenie portu(Discard Disable)

Trzeci tryb oferuje najsłabszy mechanizm zabezpieczeń, po podłączeniu do portu przełącznika nowego urządzenia, ruch od niego nie tylko nie zostanie przekazany, ale także nastąpi wyłączenie portu. Dopóki administrator nie włączy portu cały ruch na tym porcie będzie zablokowany.

Aby włączyć przypisywanie adresów MAC do portów przełącznika, należy przejść do zakładki Security -> Multiple Host i uruchomić funkcję Enable przy portach do których mają zostać przypisane konkretne adresy MAC. Kolejnym krokiem jest określenie rodzaju zamka i zablokowanie poszczególnych portów. W tym celu przenosimy się do zakładki Security -> Port Security. Wybieramy właściwy dla naszego rozwiązania tryb zamknięcia interfejsu czyli Classic Lock lub Dynamic Lock. W trybie Dynamic Lock w polu Max Entries określamy ile adresów może zostać poznanych na danym interfejsie. Następnie określamy rodzaj akcji przy złamaniu zamka czyli Access on Violation, zamykamy interfejs przez zaznaczenie pola Lock Interface, klikamy na Update i zapisujemy zmiany. Poniżej zamieszczono graficzną prezentację włączania blokady Classic Lock na porcie e1.

Interface	e1	←	Nr interfejsu
Lock Interface	<input checked="" type="checkbox"/>	←	Zamknij interfejs
Learning Mode	Classic Lock	←	Tryb zamka
Max Entries	1	←	Ilość adresów MAC
Action on Violation	Discard	←	Akcja przy złamaniu zamka
Enable Trap	<input type="checkbox"/>		
Trap Frequency	10		

W ten sposób do interfejsu e1 został przypisany MAC adres komputera, który jest podłączony do tego interfejsu.

### 2.2.7 Quality of Service

Quality of Service, czyli zapewnianie jakości obsługi na określonym poziomie. Mechanizmy QoS pozwalają na priorytetyzację jednego rodzaju ruchu ponad innym, a także przypisywanie dostępnego pasma do konkretnych portów switcha. Dzięki

zastosowaniu mechanizmów QoS już na poziomie przełącznika, nasze połączenie internetowe nie będzie obciążone przez niechciany, lub mniej ważny ruch. Dobrą praktyką jest ograniczanie pasma w większym stopniu dla normalnych użytkowników, oraz nie ograniczanie dla użytkowników wymagających stałej przepływności, lub wrażliwych na opóźnienia, takich jak ruch VoIP lub wideokonferencje.

### 2.2.7.1 Zarządzanie kolejkami

Przełącznik oferuje użytkownikowi szereg funkcji związanych z mechanizmami QoS. Część z funkcji związana jest z architekturą stosowaną w sieciach IP do zapewniania jakości usług na określonym poziomie dla danych klas ruchowych. Aktualnie w sieciach IP wdraża się głównie dwa rodzaje architektur:

- Architektura usług zintegrowanych – IntServ, pozwala na wyróżnianie strumieni ruchu dla poszczególnych protokołów sieciowych, od punktu źródłowego do docelowego, rozpoznanie danego strumienia odbywa się przy użyciu nadawania poszczególnym klasom ruchowym etykiet właściwych dla danej klasy.
- Architektura usług zróżnicowanych – DiffServ, w tym rozwiązaniu pakiety należące do różnych klas ruchu są rozróżniane przy wykorzystaniu zmodyfikowanego pola ToS (Type of Service) w nagłówku pakietów sieci IP. Na podstawie ToS stworzono pole DSCP (Differentiated Service Code Point), dzięki temu każdy z pakietów może zostać przypisany do jednej z 64 klas. Ruch który należy do klasy o wyższym priorytecie będzie przesyłany jako pierwszy.

Poszczególne z ustawień pozwalają na klasyfikację poszczególnych z pakietów, zarządzanie kolejkami na przełączniku, a także przypisywanie wag do poszczególnych klas ruchowych. W zakładce QoS-> CoS Settings mamy możliwość przypisywania do którejś z klas ruchowych (0-7) ruchu generowanego na poszczególnych portach przełącznika. Klasa 0 to klasa o najmniejszym priorytecie, a klasa 7 to ruch o najwyższym priorytecie. Oprócz przypisywania ruchu z konkretnego portu do klasy, możemy zarządzać kolejkami. Przełącznik obsługuje 4 kolejki, do których możemy przypisać konkretne klasy ruchowe. Ustawienie Class of Service definiujemy w zakładce CoS Settings a ustawienie klas na podstawie parametru DSCP w zakładce DSCP Settings.

### 2.2.7.2 Zarządzanie pasmem

Podstawowe funkcje zarządzania pasmem nie wymagają od użytkownika wiedzy na temat architektur usług IntServ lub DiffServ. Zarządzanie pasmem odbywa się w zakładce QoS -> Bandwidth Management. W tej zakładce administrator ma możliwość przypisania konkretnego pasma dla poszczególnych portów fizycznych na

przełączniku. Sterowanie pasmem odbywa się w zakresie od 62-100000 Kb/s dla ruchu wchodzącego do interfejsu, oraz w zakresie 64-100000 Kb/s dla ruchu wychodzącego z interfejsu.

<<Previous 1 2 3 Next>>

Interface

Ingress Rate Limit Status

Egress Shaping Rate on Selected Port

Committed Information Rate(CIR)

Committed Burst Size(CbS)

Port  e1  LAG

128 ← Ruch wchodzący

256 ← Ruch wychodzący

Update

Port	Ingress Rate Limit		Egress Shaping Rates		
	Status	Rate Limit	Status	CIR	CbS
e1	Enable	128	Enable	256	

Powyższy rysunek przedstawia konfigurację zarządzania pasmem na interfejsie e1, dla ruchu wchodzącego przypisano 128 Kb/s, a dla ruchu wychodzącego 256 Kb/s.

### 2.2.8 Administracja

Przełącznik oferuje administratorowi dużo funkcji wspomagających i pozwalających na łatwe zarządzanie urządzeniem. Pierwsza i jedna z najważniejszych zakładki w części Admin pozwala na dodawanie kont dla nowych użytkowników(mających dostęp do panelu zarządzania switchem). W zależności od stopnia zaawansowania naszej sieci mamy do wyboru różne tryby uwierzytelniania, podstawowym i jednocześnie najprostszym z trybów jest uwierzytelnianie lokalne. Po wpisaniu w przeglądarce adresu przełącznika, wyskoczy monit pytający użytkownika o jego nazwę oraz hasło. Bardziej zaawansowane systemy pozwalają na wykorzystanie do tego celu zewnętrznych serwerów RADIUS lub TACACS, które w tym wypadku będą zawierały dane użytkowników mających dostęp do urządzenia.

**UWAGA! W celu zwiększenia bezpieczeństwa należy zmienić domyślną nazwę użytkownika i hasło. Nieautoryzowany użytkownik może łatwo zgadnąć domyślne hasło oraz nazwę.**

Aby zmienić domyślne hasło, lub dodać nowego użytkownika należy przejść do zakładki Admin -> User Authentication. Należy wybrać typ uwierzytelniania, w podstawowej i domyślnej wersji jako Local. Następnie wpisujemy nazwę użytkownika i hasło następnie klikamy Add to List i zapisujemy zmiany. Po dopisaniu użytkownika

mamy możliwość skasowania konta domyślnego. W tym celu klikamy na konto w tabeli, domyślna nazwa konta to admin, a następnie klikamy delete i zapisujemy ustawienia. W ten sposób uzyskujemy pewność, że do konfiguracji naszego przełącznika nie będą miały dostępu postronne osoby.

### 2.2.8.1 Przypisywanie stałych adresów MAC do interfejsów

Automatycznie, switch uczy się, poprzez dodawanie adresów MAC, podłączonych do niego urządzeń sieciowych do swojej tablicy adresacyjnej. W ten sposób w momencie nadejścia ramki skierowanej do komputera o określonym adresie MAC, przełącznik sprawdza, na którym porcie podłączony jest komputer o takim adresie. Administrator ma możliwość wymuszenia na przełączniku konieczności wysyłania ramki o określonym adresie docelowym na konkretny interfejs fizyczny.

The screenshot shows a configuration form with the following fields and options:

- Interface:** Radio buttons for **Port** (selected) and **LAG**. A dropdown menu shows **e1** for Port and **1** for LAG.
- MAC Address:** An empty text input field.
- VLAN ID:** Radio buttons for **VLAN ID** (selected) and **VLAN NAME**. A dropdown menu shows **1**.
- VLAN NAME:** A dropdown menu showing **pracownia\_A**.
- Status:** A dropdown menu showing **Permanent**.
- Add to List:** A button at the bottom right.

Aby przypisać adres MAC na stałe do konkretnego interfejsu należy wybrać interfejs do którego ma zostać przypisany MAC, wpisać adres MAC, określić VLAN do którego należy dany interfejs, wybrać typ przypisania: na stałe(Permanent), do pierwszego Resetu urządzenia>Delete on Reset), do upłynięcia określonego czasu>Delete on Timeout) lub do portu który wcześniej został ustawiony w tryb Locked(Secure).

Dodatkowo użytkownik ma możliwość śledzenia aktualnej tablicy hostów, które poznał switch w trybie automatycznym. Tablice poznanych adresów MAC możemy wyświetlić w zakładce Admin - > Dynamic Address.

### 2.2.8.2 Funkcja port mirroring

W celu monitorowania i likwidacji uszkodzeń sieci niezbędne może okazać się śledzenie zawartości przesyłanej na poszczególnych portach. W momencie zauważenia zwiększonego ruchu na jednym z portów w dłuższym okresie czasu, istnieje możliwość podejrzenia jaka zawartość przechodzi przez dany port. Wykorzystujemy się do tego celu funkcję Port Mirroring. Umożliwia ona przesłanie zawartości z konkretnego portu na zupełnie inny port, do którego jest na przykład podłączony komputer zarządzający. W ten sposób po uruchomieniu na komputerze

zarządzającym programem do analizy pakietów i ramek np. EtheReal, mamy możliwość śledzenia zawartości przekazywanej przez poszczególne porty. Aby uruchomić funkcję Port Mirroring należy przejść do zakładki Admin -> Port Mirroring. Wybrać port, z którego ruch ma być przekazywany(source port), wybrać kierunek transmisji: Rx – dane odbierane, Tx – dane wysyłane, Both – przekazanie ruchu przesyłanego w obu kierunkach oraz nr portu na który ma zostać przekazana zawartość.

Source Port	e1 ▼
Type	Both ▼
Target Port	e2 ▼

Na powyższym rysunku przedstawiono sytuację, gdy ruch, zarówno wchodzący jak i wychodzący na port e1, jest przekazywany na port e2.

### 2.2.8.3 Testowanie okablowania

Oprogramowanie przełącznika pozwala na podstawowe testowanie okablowania strukturalnego podłączonego do urządzenia. Dzięki takiemu rozwiązaniu, administrator w pierwszej fazie poszukiwania uszkodzeń ma możliwość stwierdzenia na którym kablu ethernetowym występuje błąd, typu uszkodzenia oraz przybliżonej odległości do miejsca uszkodzenia.

Aby przetestować kabel sieciowy, należy kliknąć przycisk TEST umieszczony obok interesującego nas interfejsu.

e18	OK		02-Jan-2000 03:27:49	Test	Advanced
e19	No Cable	0	02-Jan-2000 03:27:46	Test	Advanced

Dodatkowo dla interfejsów typu gigabit użytkownik dysponuje jeszcze dokładniejszym narzędziem testującym pozwalającym na sprawdzenie szczegółowych parametrów badanego kabla sieciowego (jak na przykład polaryzacja kabla, lub odległość do uszkodzenia na poszczególnych parach w skrętce).

### 2.2.8.4 Tworzenie zapasowej konfiguracji

Stworzenie działającej konfiguracji na przełączniku, włączając w to VLANy, lub chociażby przypisanie do konkretnych interfejsów fizycznych adresów MAC może zająć nawet wprawnemu administratorowi dosyć dużo czasu. W celu uniknięcia konieczności ponownej konfiguracji, przełącznik daje możliwość utworzenia zapasowej kopii konfiguracji. Aby wykonać kopię zapasową pliku konfiguracyjnego należy przejść do zakładki Admin -> Save Configuration. Konfigurację możemy zapisać przy użyciu dwóch trybów poprzez protokół TFTP oraz przy użyciu http (drugi sposób jest znacznie prostszy, wystarczy wskazać docelowy katalog na komputerze z którego łączymy się ze przełącznikiem).

UPGRADE  BACKUP

File Type

Configuration

TFTP Server

Source File

Destination File

startupCfg.cfg

Proceed



Zadaniem użytkownika jest wybór trybu: upgrade pliku konfiguracyjnego, lub zapis konfiguracji jako backup.

### 2.2.8.5 Upgrade oprogramowania

Linksys cały czas udoskonala swoje produkty, najprostszym sposobem uzyskania dostępu do nowych funkcjonalności jest aktualizacja oprogramowania. Przełącznik oferuje użytkownikowi kilka trybów aktualizacji oprogramowania, dwa tryby dostępne są z poziomu przeglądarki WWW i analogiczne do trybu tworzenia i importu plików konfiguracyjnych. Użytkownik ma więc dostępne tryby upgrade przez protokół tftp oraz http. Czasami aktualizacja oprogramowania, przy wykorzystaniu narzędzi dostępnych z poziomu przeglądarki WWW nie udaje się(przyczyną mogą być błędy w transmisji lub przerwania połączenia w trakcie aktualizacji), przełącznik wyposażony jest w tryb awaryjny, dostępny poprzez port konsoli(konfiguracja przełącznika poprzez port konsoli opisana została w rozdziale 2.3).

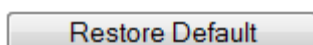
**UWAGA! Należy używać tylko oprogramowania dostarczonego przez firmę LINKSYS na stronach [www.linksys.com](http://www.linksys.com), lub [www.fen.pl](http://www.fen.pl). Wgranie do urządzenia nie właściwego firmwaru może spowodować błędne działanie, a nawet uszkodzenie przełącznika. Przed wgraniem oprogramowania należy sprawdzić wersję sprzętową urządzenia(jeżeli na obudowie nie ma dodatkowego opisu np. v1.1 mamy do czynienia z wersją 1.0). Nie należy odłączać przełącznika od zasilania w trakcie aktualizacji oprogramowania, może to spowodować niewłaściwe działanie przełącznika.**

Aby dokonać aktualizacji oprogramowania należy ściągnąć firmware ze strony producenta. Po zapisaniu pliku na komputerze zarządzającym, możemy przystąpić do aktualizacji. Upgrade przez interfejs www został opisany przy okazji tworzenia kopii zapasowej pliku konfiguracyjnego.

### 2.2.8.6 Przywracanie ustawień fabrycznych

Czasami błędna konfiguracja może powodować niewłaściwe działanie przełącznika, konieczne może okazać się przywrócenie przełącznika do ustawień fabrycznych. Aby przywrócić przełącznik do ustawień fabrycznych należy przejść do zakładki Admin -> Factory Reset.

**The Restore button returns device to Factory Default Settings.**



Po kliknięciu przycisku Restore Default należy po chwili wyłączyć i ponownie włączyć przełącznik, możemy to zrobić wyciągając wtyczkę z gniazdka elektrycznego, lub przechodząc do zakładki Admin -> Reboot i klikając przycisk Reboot.

## 2.2.8.7 Logi systemowe

Administrator ma możliwość śledzenia poszczególnych wydarzeń systemowych(logów). Zdarzenia systemowe mogą być wyświetlane w czasie rzeczywistym, przesyłane na zewnętrzny serwer syslog, lub zapisywane w jednej z pamięci przełącznika(użytkownik może zdecydować, w której pamięci mają być zapisywane wydarzenia: RAM – pamięć ulotna, po ponownym uruchomieniu logi są tracone, Flash – pamięć stała logi są zapisane nawet w przypadku odłączenia zasilania).

Można wyróżnić kilka rodzajów logów, użytkownik decyduje które z nich mają zostać zapisane w pamięci przełącznika.

Severity	Memory Logs	Flash Logs
Emergency	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Alert	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Critical	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Error	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Warning	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Notice	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Informational	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Debug	<input type="checkbox"/>	<input type="checkbox"/>

**System przestał funkcjonować**  
**System wymaga natychmiastowej interwencji**  
**System jest w stanie krytycznym**  
**Wystąpił błąd systemowy**  
**Wystąpiło ostrzeżenie systemowe**  
**System działa właściwie, ale wystąpiło zdarzenie**  
**Informacja o urządzeniu**  
**Wystąpił błąd w systemie zdarzeń**

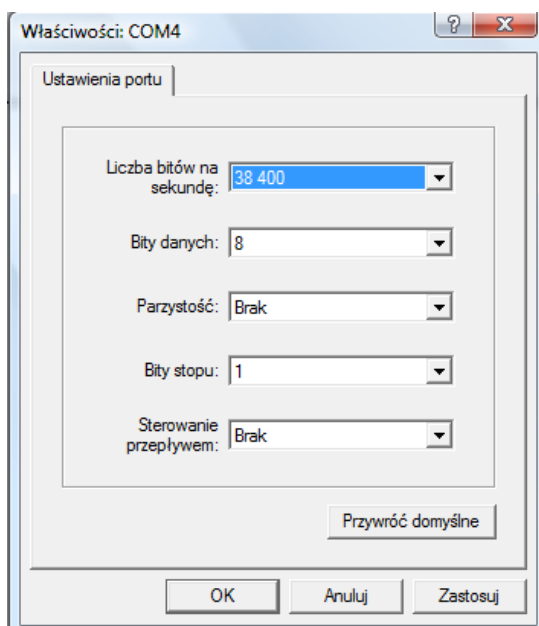
Po zdecydowaniu, które z logów mają być zapisywane do pamięci mamy możliwość śledzenia zdarzeń w zakładce Admin -> Memory Logs, lub Admin -> Flash Logs w zależności od tego które logi chcemy wyświetlać. Dodatkowo w zakładce Admin -> Server Logs możemy ustawić zrzucanie logów.

Na poniższym rysunku zamieszczono przykładowe zdarzenia systemowe. Jak można zauważyć, przy normalnej pracy systemu informowani jesteśmy o podstawowych sprawach jak logowanie się użytkownika do urządzenia, włączenie lub wyłączenie interfejsu.

Log Index	Log Time	Severity	Description
1	2147483612	01-Jan-2000 01:04:45	Informational %AAA-I-CONNECT: New http connection for user admin, source 192.168.3.44 destination 192.168.3.78 ACCEPTED
2	2147483613	01-Jan-2000 01:04:19	Informational %BOOTP_DHCP_CL-I-DHCPCONFIGURED: The device has been configured on interface Vlan 1, IP 192.168.3.78, mask 255.255.255.0, DHCP server 192.168.3.1
3	2147483614	01-Jan-2000 01:03:58	Informational %AAA-I-CONNECT: User CLI session for user admin over console, source 0.0.0.0 destination 0.0.0.0 ACCEPTED
4	2147483615	01-Jan-2000 01:01:28	Informational %Box-I-SFP-PRESENT-CHNG: SFP# 2 changed to - not present.
5	2147483616	01-Jan-2000 01:01:27	Informational %Box-I-SFP-PRESENT-CHNG: SFP# 1 changed to - not present.
6	2147483617	01-Jan-2000 01:01:16	Warning %LINK-W-Down: g4
7	2147483618	01-Jan-2000 01:01:16	Warning %LINK-W-Down: g3
8	2147483619	01-Jan-2000 01:01:16	Warning %LINK-W-Down: g2

## 2.3 Konfiguracja przełącznika przez port konsoli

Zarządzanie przez port konsoli wykorzystuje do komunikacji z przełącznikiem połączenie szeregowe, w które standardowo wyposażone są komputery klasy PC. Ten tryb połączenia może okazać się koniecznym w przypadku wgrania do urządzenia uszkodzonego oprogramowania, lub utraty haseł do interfejsu zarządzania. Każdy z przełączników zarządzalnych wyposażony jest w port RS-232 przeznaczony do połączenia konsolowego. Wraz z przełącznikiem, Linksys dostarcza kabel dedykowany do zestawienia takiego połączenia. Dodatkowo w celu zestawienia połączenia należy wykorzystać program wbudowany w system operacyjny Windows XP. Jeżeli system na którym pracujemy nie ma wbudowanego oprogramowania, możemy ściągnąć oprogramowanie ze strony [www.hilgraeve.com/htpc.html](http://www.hilgraeve.com/htpc.html). Oprogramowanie HyperTerminal jest darmowe dla użytkowników nie komercyjnych. Aby właściwie zestawić połączenie między przełącznikiem a komputerem, należy wybrać nr portu do którego podłączony jest przełącznik(domyślnie to COM1), a następnie wprowadzić w programie poniższe ustawienia:



Po wprowadzeniu ustawień i kliknięciu ok zobaczymy ekran połączenia, po wciśnięciu Enter pojawi się ekran uwierzytelniania.

**Login Screen**

=====

User Name: XXXXXXXXXX

Password:

---

Po wybraniu Edit wpisujemy domyślne(lub ustawione przez siebie) nazwę użytkownika i hasło, wciskamy klawisz Esc, wybieramy Execute i wciskamy Enter. Jeżeli nazwa użytkownika i hasło zgadzają się z zamieszczonymi w konfiguracji przełącznika, uzyskamy dostęp do panelu konfiguracyjnego.

### Switch Main Menu =====

#### **1. System Configuration Menu**

- 2. Port Status
- 3. Port Configuration
- 4. Help
- 0. logout

Główny panel konfiguracyjny daje możliwość przejścia do bardziej zaawansowanej konfiguracji urządzenia, wyświetlenia statusu poszczególnych portów, podstawowej konfiguracji poszczególnych portów, wyświetlenia pomocy, a także zakończenia sesji konfiguracyjnej

### 2.3.1 Konfiguracja podstawowych funkcji

Podstawowe ustawienia dostępne są w System Configuration Menu.

### System Configuration Menu =====

- 1. System Information**
- 2. Management Settings
- 3. User & Password Settings
- 4. Security Settings
- 5. IP Configuration
- 6. File Management
- 7. Restore System Default Settings
- 8. Reboot System
- 0. Back to main menu

Użytkownik ma możliwość wyświetlenia:

- Informacji o systemie(wersja oprogramowania, MAC, nazwa)
- Informacji zarządzających(konfiguracja połączenia szeregowego, protokołu Telnet)
- Ustawienia użytkowników i haseł

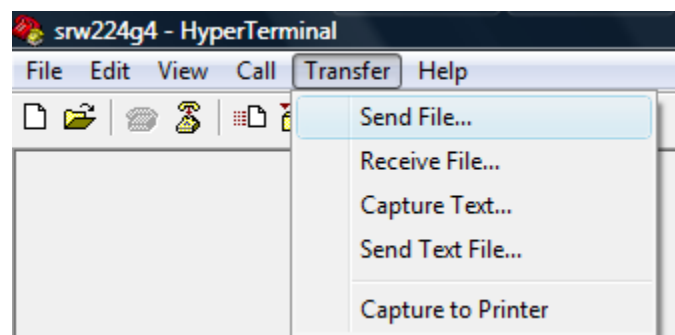


- [4] wejścia do trybu diagnostycznego
- [5] ustawienie prędkości połączenia szeregowego

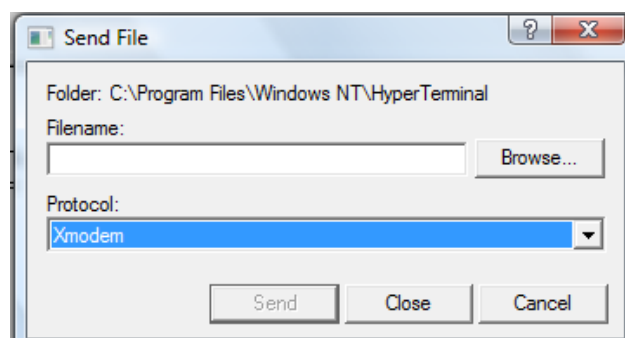
Aby wgrać nowy firmware przy użyciu trybu awaryjnego należy wybrać opcję 1. Po wybraniu opcji pojawi się komunikat:

```
Startup Menu
[1] Download Software
[2] Erase Flash File
[3] Password Recovery Procedure
[4] Enter Diagnostic Mode
[5] Set Terminal Baud-Rate
[6] Back
Enter your choice or press 'ESC' to exit:
Downloading code using XMODEM.
$$$$$$_
```

Urządzenie oczekuje teraz na wgranie nowego oprogramowania. Wgrywanie nowego oprogramowania z wykorzystaniem połączenia konsolowego odbywa się przez protokół xmodem wbudowany w program HyperTerminal. Aby przesać oprogramowanie do przełącznika poprzez xmodem należy wybrać z zakładki programu HyperTerminal Transfer-> Wyślij plik(Send File):



Następnie wybrać w polu Protocol -> Xmodem, wskazać plik który ma zostać wysłany(oprogramowanie dostępne na stronie producenta), a następnie kliknąć wyślij(Send).



---

Aktualizacja oprogramowania z wykorzystaniem połączenia szeregowego może zająć około pół godziny. W tym czasie nie należy odłączać przełącznika od źródła zasilania.

Po wybraniu opcji 3 możemy przejść do procedury odzyskiwania haseł, użytkownik ma możliwość nadpisania istniejącego hasła.

Pozostałe elementy trybu awaryjnego nie powinny być wykorzystywane bez dokładnej znajomości poszczególnych z nich. W celu zapoznania się z pozostałymi funkcjami prosimy o zapoznanie się z podręcznikiem obsługi dedykowanym do tego urządzenia.

---

# Gwarancja:

Konsorcjum FEN Sp. z o.o. prowadzi serwis gwarancyjny produktów oferowanych w serwisie dealerskim [www.fen.pl](http://www.fen.pl).

Procedury dotyczące przyjmowania urządzeń do serwisu są odwrotne do kanału sprzedaży tzn.: w przypadku uszkodzenia urządzenia przez klienta końcowego, musi on dostarczyć produkt do miejsca jego zakupu.

## Skrócone zasady reklamacji sprzętu:

Reklamowany sprzęt powinien być dostarczony w stanie kompletnym, w oryginalnym opakowaniu zabezpieczającym lub w opakowaniu zastępczym zapewniającym bezpieczne warunki transportu i przechowywania analogicznie do warunków zapewnianych przez opakowanie fabryczne.

Szczegółowe informacje dotyczące serwisu można znaleźć pod adresem [www.fen.pl/serwis](http://www.fen.pl/serwis)

Konsorcjum FEN współpracuje z Europejską Platformą Recyklingu ERP w sprawie zbiórki zużytego sprzętu elektrycznego i elektronicznego. Lista punktów, w których można zostawiać niepotrzebne produkty znajduje się pod adresem [www.fen.pl/download/ListazSEIE.pdf](http://www.fen.pl/download/ListazSEIE.pdf)

## Informacja o przepisach dotyczących ochrony środowiska

Dyrektywa Europejska 2002/96/EC wymaga, aby sprzęt oznaczony symbolem znajdującym się na produkcie i/lub jego opakowaniu ("przekreślony śmietnik") nie był wyrzucany razem z innymi niesortowanymi odpadami komunalnymi. Symbol ten wskazuje, że produkt nie powinien być usuwany razem ze zwykłymi odpadami z gospodarstw domowych. Na Państwu spoczywa obowiązek wyrzucania tego i innych urządzeń elektrycznych oraz elektronicznych w wyznaczonych punktach odbioru. Pozbywanie się sprzętu we właściwy sposób i jego recykling pomogą zapobiec potencjalnie negatywnym konsekwencjom dla środowiska i zdrowia ludzkiego. W celu uzyskania szczegółowych informacji o usuwaniu starego sprzętu prosimy się zwrócić do lokalnych władz, służb oczyszczania miasta lub sklepu, w którym produkt został nabyty.

**Powyższa instrukcja jest własnością Konsorcjum FEN Sp. z o.o.**



Dział Wsparcia Technicznego

Konsorcjum FEN Sp. z o.o.

Kontakt: [help@fen.pl](mailto:help@fen.pl)

Importer i dystrybutor: Konsorcjum FEN Sp. z o.o., ul. Dąbrowskiego 273A, 60-406 Poznań  
e-mail: [sales@fen.pl](mailto:sales@fen.pl); [www.fen.pl](http://www.fen.pl)

