

# **S m a r t S w i t c h 8P POE**

**8 портов 10/100 Ethernet свитч**  
**с възможност за добавяне на PoE модул**  
**и**  
**конфигуриране и управление от *PicoIP***

***Ръководство на потребителя***

# СЪДЪРЖАНИЕ

1. Версии на документа.....	3
2. Въведение.....	4
3. Основни функции и параметри SS8P.....	5
3.1. Стандартни функции.....	5
3.2. Допълнителни функции, достъпни през PicoIP.....	5
3.3. Указания за използване на вградените газоразрядници (от версия DW208R_D4).....	5
3.4. Указания за използване на PoE функциите на SS-208POE.....	7
3.5. Технически параметри.....	9
4. Сравнение между RTL8309SB и RTL8309G.....	10
5. Свързване на PicoIP към SS8P.....	11
6. Достъп до параметрите на SS8P.....	12
6.1. Достъп през Web.....	12
6.2. Достъп през SNMP.....	12
6.3. Функция “Smart Configuration Apply”.....	12
7. Кратко описание на функциите на SS8P.....	14
7.1. Настройки и статус на портовете („Port Status“)......	14
7.2. Глобални настройки („Global Settings“)......	15
7.3. Порт и таг-базирани VLAN („VLAN“)......	16
7.4. Търсене в MAC таблицата („MAC Search“)......	18
7.5. Съхраняване на конфигурация на SS8P във файл („Save Config“)......	18
7.6. Зареждане на конфигурацията на SS8P от файл („Load Config“)......	18
7.7. Зареждане на фабрични настройки в SS8P („Default“)......	19
7.8. Рестартиране на SS8P („Restart“)......	19
7.9. Параметри на SS8P , достъпни за конфигуриране с джъмperi.....	19
7.9.1 „Broadcast storming“ или контрол на “broadcast” трафика.....	19
7.9.2 „Port trunking“ .....	19
7.9.3 „Max frame size 1552 bytes“ .....	20
8. Решаване на конкретни VLAN задачи с SS8P.....	21
8.1. Порт-базиран VLAN: “всички портове виждат един, без да се виждат по между си”.....	21
8.2. Порт-базиран VLAN: Разделяне на SS8P на два логически 4—портови суитча.....	22
8.3. Таг-базиран VLAN: Отделяне на до 802.1q трафик към конкретни портове без tag/untag.....	23
8.4. Таг-базиран VLAN: Свързване на untag клиент към 802.1q мрежа.....	24
9. Параметър “Broadcast Drop Mode”.....	26

## Легенда:



Текстът съдържа допълнителна и полезна информация, която разяснява специфични ситуации и особености.



Текстът съдържа информация от съществена важност, която непременно трябва да се прочете!

## 1. Версии на документа

Версия	Дата	Кратко описание на въведените промени
2.11	18.02.10	Добавена информация за вградената клемма за PoE
2.10	22.10.09	Добавен раздел 3.4 за SS8P-POE Добавен раздел 4 за RTL8309G
2.03	18.02.09	Добавен раздел 3.3 за версия _D4
2.02	29.09.08	Добавени бележки в раздел 4
2.01	10.06.08	Добавена бележка в раздел 5
2.00	1.02.08	Изцяло обновена версия на документа с подробни описания и примери
1.00	-	Начална версия на документа

## 2. Въведение

**SS8P** е мрежов комутатор за 10/100 Ethernet мрежи с ниска консумация на енергия и набор от допълнителни функции и параметри за конфигуриране. Дизайнът му е направен с цел лесно присъединяване към управляващ IP модул (*PicoIP*) и вграждане на „PoE“ конвертор, който да осигури директното захранване на суитча от магистралното напрежение. Основните техн. параметри на **SS8P** са:

- ✓ „PoE“ възможности
- ✓ Гарантиран стартов ток от 26mA с RTL8309G (35mA с RTL8309SB)!
- ✓ Изключително ниска консумация на енергия: макс. 2.5W при пълно натоварване;
- ✓ 1K MAC таблица;
- ✓ 9 VLAN групи;
- ✓ Възможност за порт-базиран и таг-базиран VLAN;
- ✓ Възможност за тагване/разтагване на 802.1q VLAN трафик;
- ✓ QoS с две нива на приоритет и три критерия;
- ✓ Статус на портовете (вкл. Link Quality);
- ✓ и др.



Без наличието на управляващ *PicoIP* модул **SS8P** може да се използва само като обикновен суитч в 10/100 LAN мрежи. Свързването му към *PicoIP* позволява да се получи достъп до допълнителните му функции. Когато *PicoIP* остава постоянно свързан към **SS8P** това превръща двете устройства в управляем суитч (*PicoIP* дава достъпа по IP адрес да конфигурацията на **SS8P**).

Възможно е и използването на *PicoIP* само като „програмиращ“ модул, чрез който да получите достъп до параметрите на **SS8P**, но като цяло да няма необходимост от постоянен достъп и възможност за тяхната промяна в последствие. Така, след въвеждане на необходимата конфигурация в **SS8P**, се премахва *PicoIP*, а **SS8P** запазва в енергонезависима памет своята конфигурация.

### 3. Основни функции и параметри *SS8P*

#### 3.1. Стандартни функции

- “PoE” конектор за добавяне на захранващ модул, чрез който SmartSwitch може да се захранва директно през RJ45 от магистралното напрежение
- Два PE (PowerEnabled) порта
- Вградена винтова клемма на платката за въвеждане/извеждане на магистралното напрежение
- GreenEthernet – намаляване консумацията на енергия според дължината на UTP кабелите (само RTL8309G)
- “Изключване” на портовете, на които няма връзка (PowerDown)
- 8 портове 10/100Base T/TX Nway (Auto-negotiation) суитч с екранирани RJ-45 конектори;
- Изключително ниска консумация на енергия – оптимално решение за PoE системи;
- Автоматично „научаване“ на мрежовата топология;
- Автоматично разпознаване на „Full“/“Half“ дуплекс режим;
- Гарантирана 200Mbps честотна лента на всеки порт;
- „Store & Forward“ метод на обработка на фреймовете
- „IEEE 802.3x flow control“ при Full-duplex;
- „Zero-Packet Loss Back-pressure flow control“ при Half-duplex
- Индикатори (LEDs): Power и Link/Activity
- Поддръжка на “Auto MDIX” на всеки порт

#### 3.2. Допълнителни функции, достъпни през *PicoIP*

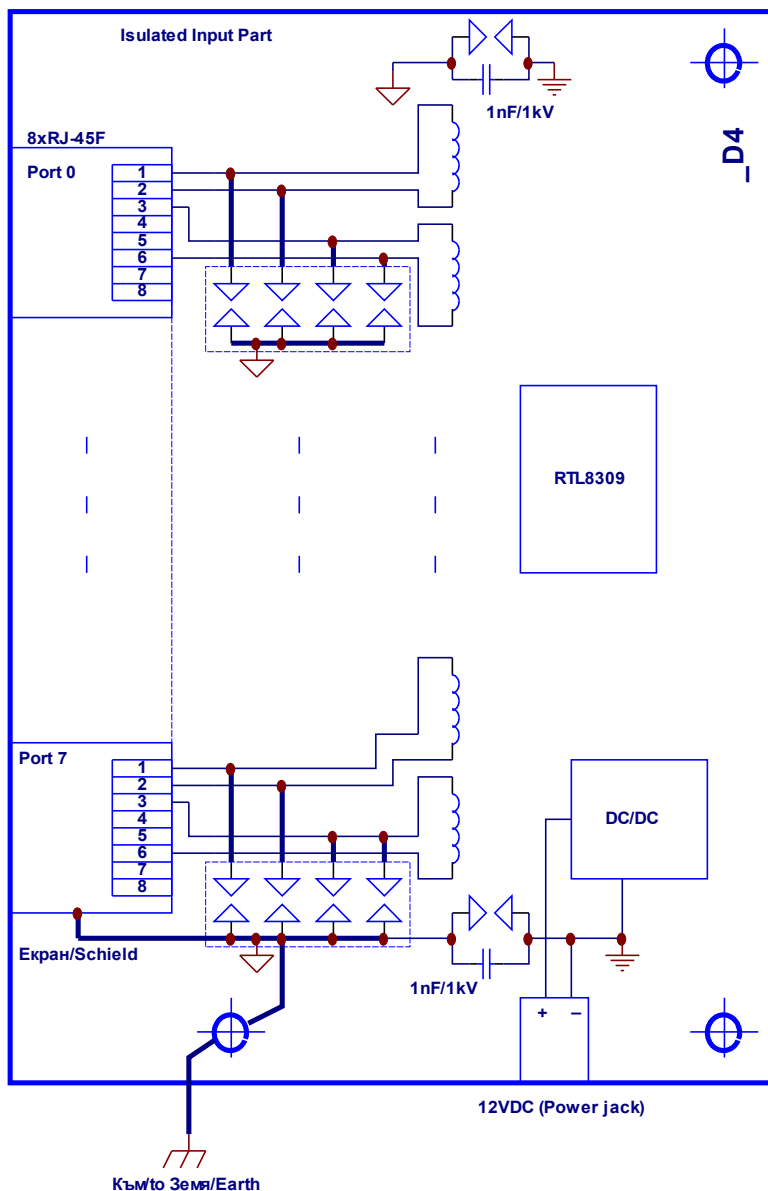
- Порт-базирано VLAN групиране в 8 групи;
- QoS:
  - Две нива на приоритет с настройваеми съотношения;
  - Критерии на приоритетизация: Номер на порт, 802.1p tag, TCP/IP DiffServ, Клас от IP адреси;
- 802.1q порт/tag базиран VLAN;
- Възможност за вмъкване/премахване на 802.1q тагове на всеки порт;
- Настройваемо време на обновяване на MAC таблицата (300s, 800uS);
- Детайлен статус на портовете: връзка, скорост, качество на връзката, Loop и др.
- Възможност за спиране/пускане на всеки порт по отделно;
- Функция „Broadcast Storming“ (чрез джъмпер);
- Функция „Packet size 1552 bytes“ (чрез джъмпер);
- Функция „Port trunking“ на два порта (чрез джъмпер);

#### 3.3. Указания за използване на вградените газоразрядници (от версия *DW208R\_D4*)

В новата версия (DW-208R\_D4) на „НЕОМОНТАНА ЕЛЕКТРОНИКС“ на SmartSwitch за първи път в този клас продукти са фабрично вградени 24бр. печатни газоразрядници на всички сигнални проводници от RJ-45 портовете. Предназначението им е да способстват за неутрализиране на пиковите напрежения, които съпътстват използването на суитчовете в открити/градски условия. Всеки от вградените газоразрядници има пробивно напрежение от около 1.2kV.

На фигурата е показана опростена принципна схема на SmartSwitch версия „D4“. Всички газоразрядници са свързани заедно с екрана на RJ-45 конекторите и към отворът за закрепване на платката, разположен непосредствено до конекторите. Добавени и са два разрядника в паралел на свързващите кондензатори (1nF/1kV) между екрана на входа и масата на захранването.

За да бъде ефективна защитата чрез газоразрядниците е необходимо да се заземи общият им край, като за целта най-удобно е да се използва отворът за закрепване на платката.



**Опростена принципна схема на SS8P с вградени газоразрядници**



Свързването към Земя на входната част води и до заземяване по променлив ток на масата (минусовият проводник) на захранването. При използване на DC/DC импулсно захранване на суитча това води и до заземяване по променлив ток на минуса на цялата захранваща верига.



При използване на два насрещни SS8P\_D4 с връзка между тях по FTP е препоръчително екранът на FTP кабела да се свърже към екрана само на единия SS8P\_D4 (с екранирано RJ-45). По този начин се избягва протичането на изравнителни токове по екрана на FTP в следствие на потенциалните разлики в двата края на трасето.

### 3.4. Указания за използване на PoE функциите на SS-208POE

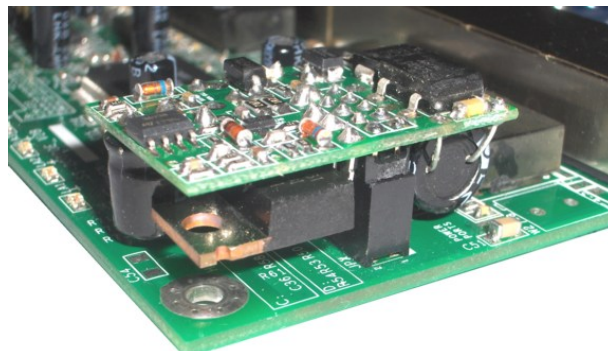
С версия SS-208POE “НЕОМОНТАНА ЕЛЕКТРОНИКС” представя уникално по рода си решение за опростено изграждане на LAN мрежи, чрез вградено захранване в *SmartSwitch*.



Разположение на новите куплунзи

Винтова клема

Куплунг за PoE модул



Монтиране на захранващия модул към куплунга

Новото в този продукт е допълнителният куплунг на платката на *SmartSwitch*, чрез който се включва захранващ модул от типа [SMPS H0C5P](#). Куплунгът е свързан със свободните двойки (4-5 и 7-8) на два от RJ-45 портовете (No. 1 и 2) и така става възможно захранването на суитча директно с подаваното през RJ-45 напрежение. Поляритетът ще е без значение, тъй-като захранващите модули са с вградени Греци изправители на входа. Диапазонът на подаваното захранващо напрежение зависи от модела на захранващия модул:

- 25-65VAC (20-95VDC) за [SMPS H0C5P](#)
- 35-85VAC (20-120VDC) за [SMPS F0C5P](#)

Захранващият модул осигурява на *SmartSwitch* необходимите за нормалната му работа 12VDC/0.5A. Това напрежение „излиза“ и на захранващото гнездо на *SmartSwitch*, от където то може да бъде изведено и използване за захранване на друг *SmartSwitch* или на управляващия *PicoIP* модул.

За по-голяма гъвкавост при различни тропологии е вградена винтова клема за въвеждане/извеждане на магистралното напрежение. Чрез нея също може да се подаде захранващо напрежение към модула без да се преминава през RJ-45 конекторите. По-този начин се избягват споменатите ограничения, които се налагат при използване на захранване през RJ-45. Клемата може да се използва и за първоначално (веднага след централното захранване) въвеждане на захранващото напрежение в свободните чифтове (т.е. първият суитч да игра ролята и на „Injector“) и така да се спестят разходи по набавяне на отделен „PoE Injector“

При реализацията на верижно свързани *SmartSwitch* чрез PoE захранване трябва да се имат предвид следните ВАЖНИ особености:



RJ-45 конекторите на *SmartSwitch* са предназначени за максимален ток 1.5A и максимално напрежение 125VAC.

В суитчовите по веригата ще тече СУМАРНИЯ ток на всички следващи суитчове!



Включването под напрежение на RJ-45, в които има захранващо напрежение НЕ Е ЖЕЛАТЕЛНО, тъй-като води до протичане на големия пусков ток през неустановения добър контакт. Този пусков ток силно намалява след първите 100м. от трасето.



Кримпването на RJ-45 под напрежение също е НЕЖЕЛАТЕЛНО поради окъсяването от клещите на всички изводи. Освен, че ще доведе до късо в захранващата магистрала, може да се получи и прехвърляне на захранващо напрежение към сигналните линии и така да се повреди отсрещното устройство.



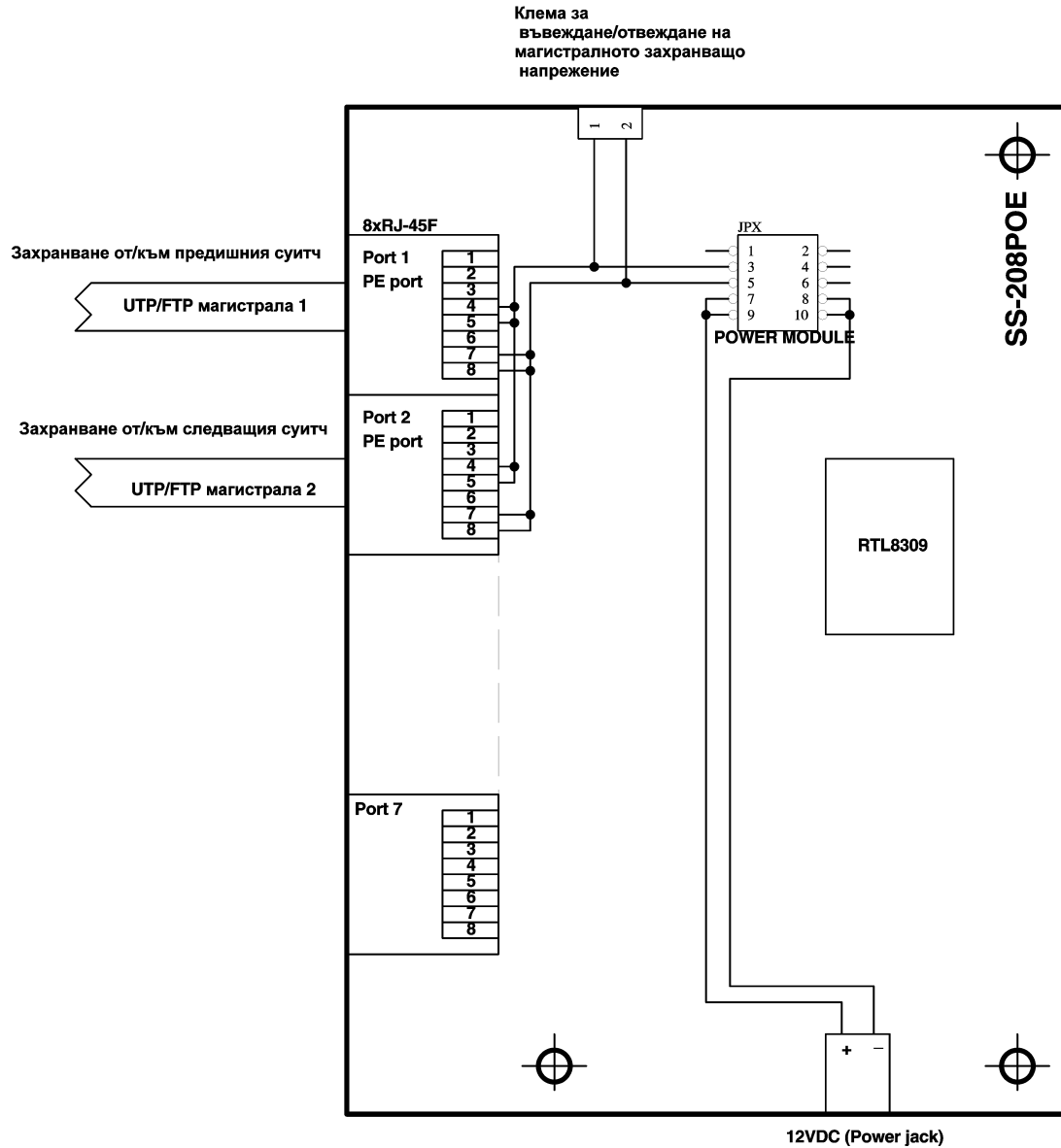
Подаването на 12VDC към SmartSwitch едновременно през PoE модул и през външно захранване (през жака) НЕ Е ДОПУСТИМО, тъй-като изходите на двете захранвания се явяват в паралел.



НЕ Е ДОПУСТИМО входния кабел със захранването да се включва в останалите портове на суитча, тъй-като в тях има маломощни товарни резисторни групи между 4-5 и 7-8.



Предлаганото решение НЕ ОТГОВАРЯ на стандартите **IEEE802.3af** за Power Over Ethernet!



Принципна схема на SmartSwitch с PoE връзките



### 3.5. Технически параметри

#### Стандарти

IEEE 802.3 10BASE-T  
IEEE 802.3u 100BASE-TX

#### Брой портове

8 интегрирани порта (10/100Mbps Nway)  
2 порта са свързани към конектора за PoE модул

#### Поддръжка на "Flow Control"

Half-duplex mode: Backpressure  
Full-duplex mode: IEEE 802.3x.


#### Медия

10Base-T Cat. 3, 4, 5 UTP/STP  
100Base-TX Cat. 5 UTP/STP

#### Индикатори

На порт: LINK/ACT (SMD LED's с ниска консумация на енергия)  
Общ: POWER

#### Захранване

- Абсолютна максимална стойност на захранващото напрежение – 15VDC !!!
- Работна стойност на захранването: 7.5VDC – 15VDC;
- Конектор: Жак (2.1mm) 

#### Консумация на енергия (@12VDC)

- Стартов ток и ток на покой (без свързани портове): <26mA за RTL8309G и <0.35mA за RTL8309SB (0.45W)
- Ток при товар (свързан порт):
  - +20mA на всеки 100Mbps порт
  - +1mA на всеки 10Mbps порт;
- Максимум: 2.4W (~190mA при пълно 100Mbps натоварване)

Работен температурен обхват: 0°~ 55°

Температура на съхранение: -20°~ 90°

Допустима влажност при употреба: 10% ~90% RH (без кондензиране)

#### 4. Сравнение между RTL8309SB и RTL8309G

RTL8309G е най-новата модификация от популярната серия 8 портови 10/100 чипове на Realtek Semiconductor. Чипът е представен в края на 2008г. и е произведен с по-съвременна 0.16 $\mu$ m технология (за разлика от 0.18 $\mu$ m при RTL8309SB).


Основната разлика във версията „G” е наличието на режим на спестяване на енергията в зависимост от дължината на кабела (GreenEthernet). Това е реализирано чрез динамично следене на дължината на кабела и съответна промяна в мощността на предаване. Същевременно е постигната и по-ниска обща консумация на самият чип. В следващата таблица е представен сравнителен анализ с приблизителни стойности между двата чипа при захранване 12V на *SmartSwitch*:


Условия на измерване	RTL8309G	RTL8309SB (модификация) <sup>1)</sup>	Подобрение
Стартов ток (без линкове)	26mA	35mA	<b>9mA</b>
100Mb линк (до 20m)	17mA на порт	21mA на порт	<b>4mA на порт</b>
100Mb линк (~150m)	21mA на порт	21mA на порт	<b>0mA на порт</b>

1) Стойностите са валидни само за чипове RTL8309SB вграждани в SmartSwitch на НЕОМОНТАНА ЕЛЕКТРОНИКС, тъй-като те са специална модификация с нисък стартов ток. При останалите 8309SB стартовият ток е 130mA!

В следващата таблица са показани няколко примера за сравнение при по-често срещаните в практиката конфигурации от дължините на кабелите и количеството спестена енергия при използване на RTL8309G:

Условия на измерване	RTL8309G	RTL8309SB	Подобрение
8x100Mb (до 20m)	163mA	197mA	<b>34mA (17%)</b>
6x100Mb (до 20m) +2x100Mb (100m)	171mA	197mA	<b>26mA (13%)</b>

 За коректната работа на SmartSwitch с RTL8309G е необходимо обновяване на системния софтуер на PicoIP до 4.084. В тази версия е подобрена комуникацията между PicoIP и SmartSwitch и ще доведе до по-стабилна работа при достъп и до суич с RTL8309SB (проблемът с получаването на некоректен статус на портовете при някои образци).

 При обновяване до 4.084 от произволна по-стара версия всички конфигурационни параметри – IP адрес, маски, режими на работа се запазват с изключение на user/password за достъп под Web (те приемат фабричните стойности admin/admin) и на AccessIP/MASK (техните фабрични стойности са „без ограничение на достъпа“).

## 5. Свързване на *PicoIP* към *SS8P*



Преди да пристъпите към свързване на устройствата първо се уверете, че имате нормален мрежов достъп до *PicoIP* (ping, SNMP/Web)!

Свързването да става при изключено захранване на устройствата!

*PicoIP* и *SS8P* са специално проектирани за съвместна работа. За целта и на двете устройства са предвидени конектори за връзка по между им, която се осъществява посредством специален кабел. Модулният дизайн позволява гъвкаво използване на двете устройства отделно и съвместно.

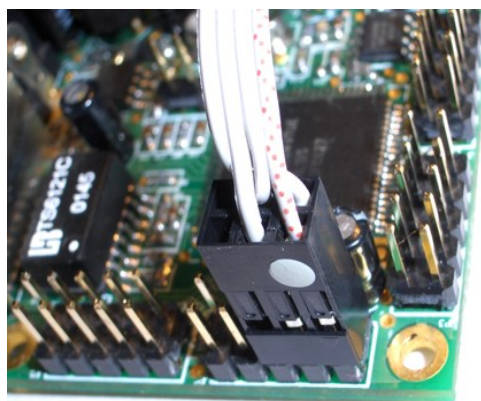
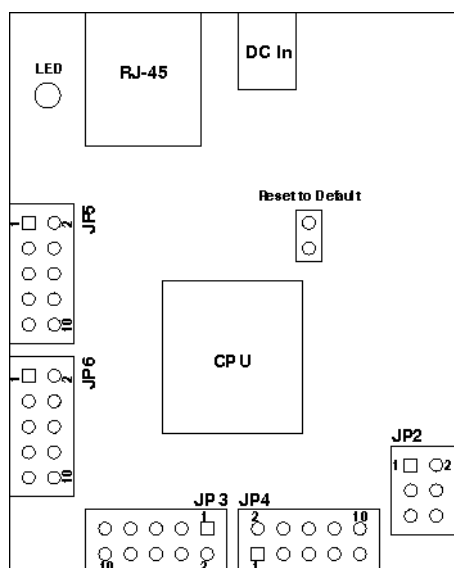


Тази връзка единствено дава възможност на *PicoIP* за контрол на *SS8P*. Тя не осигурява Ethernet линка към *PicoIP* – той трябва отделно да се свърже в мрежата чрез патч кабел.

При необходимост от постоянен “on-line” достъп за управление на *SS8P*, *PicoIP* се свързва към него и двете ползват общо захранване.

В много случай, може да е достатъчна само възможността в *SS8P* да се зареди някаква специфична конфигурация (например VLAN групиране на портовете, с цел създаване на логически сегменти). Тогава *PicoIP* модулът се използва като програматор и след зареждане на необходимата конфигурация, той се демонтира от *SS8P*. С цел лесно зареждане на една и съща конфигурация в много на брой *SS8P* в клиентските приложения, както и във Web сървъра, е предвидена възможност за съхраняване/зареждане на конфигурацията във файл.

1.) Куплунгът от страната на *PicoIP* е маркиран със сива точка. Той се поставя върху пинове 5,6,7,8,9,10 от JP6 така, че двете свободни гнезда от куплунга да съвпадат с пинове 5,6 на JP6.




2.) Другият край на кабела се поставя на конектора на *SS8P*, така че свободните му изводи да съвпадат с пинове 2 и 4.



Във фабричните настройки на *PicoIP* режимът „Switch Control” (управление на SmartSwitch) е **ИЗКЛЮЧЕН!** За да получите достъп до параметрите на SmartSwitch трябва да пуснете режима през Web или WinTIC (SNMP)!

## 6. Достъп до параметрите на SS8P


Достъпът до параметрите на *SS8P* е възможен по два начина: чрез Web браузър и връзка към Web сървъра на *PicoIP* или чрез SNMP команди. SNMP достъпът се използва и в приложението WinTIC, което улеснява използването им чрез своя визуален интерфейс.

 По подразбиране на *PicoIP* не е включен софтуерният модул за контрол на *SS8P* и менютата и SNMP командите не са достъпни. За включване на този режим е необходимо разрешаването на опцията „SmartSwitch Control Mode“, която се намира в групата „Operating modes“ в WinTIC или в менюто „Setup->Switch Control „ под Web.

При вграждане на управлението на *PicoIP* и респективно на *SS8P* във вече разработени софтуерни системи за контрол и мониторинг трябва да се използва SNMP достъпа. За него са налични множество готови софтуерни библиотеки, както и целият пакет „net-snmp“, който е с отворен код.

### 6.1. Достъп през Web

За достъп до различните параметри на *SS8P* през Web е обособена отделна категория в Web страницата на *PicoIP* – „Switch Control“. Детайлно описание на менютата е поместено в следващия раздел.

 Промяната на който и да е параметър от настройките на *SS8P* не се възприема от него мигновено - единствено се променя конфигурационната му памет. Тя се зарежда от *SS8P* само след рестартиране на суичта. За това е необходимо да се извърши рестартиране (менюто „Reboot“ в групата „Switch Control“), след като се приключи с настройките на суичта. Това важи и за случая, когато се зарежда цялостна конфигурация от бинарен файл или се зареждат фабричните настройки на суичта („Default“).

### 6.2. Достъп през SNMP

Всички описани опции за конфигуриране на *SS8P* са достъпни и през SNMP. Налични са два метода на достъп за конфигуриране – на ниско ниво и чрез разширена SNMP структура.

Достъпът на ниско ниво е съвместим с *TinyIP* и е запазен с цел обратна съвместимост. Използва се от WinTIC приложението, но е сложен за директно използване от потребителя.

Разширената SNMP структура е специално разработена за да улесни достъпа до конфигурационните параметри от потребителя. За целта е разработено изцяло нова SNMP структура с корен: enterprises.Neomontana(19865).TinyIP(1).Switch(3). Чрез нея на „високо“ ниво могат да се конфигурират основните параметри на *SS8P*.

Детайлно описание на различните OID-ове, достъпни в тази структура може да бъде намерено в съответния MIB файл: [“PicoIPRTL-MIB.txt”](#).

### 6.3. Функция “Smart Configuration Apply“

Това е специално проектирана системна функция на *PicoIP*, предназначена за предпазване от “лошо” конфигуриране на *SS8P* особено, когато към него е свързан и Ethernet линка на *PicoIP*. Такова конфигуриране би могло да прекрати достъпа до *PicoIP* модула през мрежата и да го направи изцяло недостъпен.

“Smart Configuration Apply” се грижи за това да провери дали след реконфигурирането на *SS8P* и неговия рестарт, връзката до *PicoIP* се е запазила. Проверката на връзката става, чрез достъп до специално заделен SNMP OID (rtlApply.0), който е необходимо да бъде изчетен веднъж в рамките на около 2min

след всяко рестартиране на *SS8P*, преди което е имало промяна в конфигурацията му. Невъзможността да се изчете този параметър (при липса на достъп до *PicoIP*) в рамките на този интервал води до автоматично зареждане в *SS8P* на фабричните настройки и неговото рестартиране. Това от своя страна гарантира възстановяването на достъпа до *PicoIP*.

Потвърждаването на настройките може да стане и с достъп през Web до някоя от страниците. С други думи, ако се използва Web достъп, не е необходимо да се генерира SNMP за потвърждаване, а трябва след като се рестартира суитча да се направи поне едно реално зареждане на страница от Web сървъра (например страницата за статус на протозете).



*Задействането на този механизъм временно (до изтичане на 2min или до потвърждаване на настройките по един от описаните начини) преустановява рестартирането на SmartSwitch в следствие на ICMP мониторинг събития. По този начин се предпазва SmartSwitch от рестартиране по време на конфигуриране, което може да доведе до възприемане на непълна конфигурация.*

## 7. Кратко описание на функциите на SS8P

В този раздел са описани всички налични за настройка функции и параметри на SS8P. За онагледяване е използван Web интерфейсът на PicoIP. Отделно са разгледани параметрите, които могат да се настроят с помощта на джъмperi, разположени на платката.

### 7.1. Настройки и статус на портовете („Port Status“)

Страницата показва текущото състояние на всички портове на SS8P. Тя се презарежда автоматично на всеки 10 секунди, поради което не е необходима никаква намеса от потребителя за следенето на портовете в реално време.

Port	Mode	Link	100Mb/s	Full Duplex	Remote Fault	Jabber Detect	AutoNeg. Complete	Link Quality 0=High 15=Low
1	Tx/Rx	Up	Yes	Yes	No	No	Yes	0
2	Tx/Rx	Down	-	-	-	-	-	-
3	Tx/Rx	Down	-	-	-	-	-	-
4	Tx/Rx	Down	-	-	-	-	-	-
5	Tx/Rx	Up	No	No	No	No	Yes	0
6	Tx/Rx	Down	-	-	-	-	-	-
7	Tx/Rx	Down	-	-	-	-	-	-
8	Tx/Rx	Down	-	-	-	-	-	-

Page is automatically refreshed on every 10 seconds

Страницата предоставя следната информация:

- **Port** – определя номера на порта.
- **Mode** – показва режима на работа на порта: Tx=разрешено изпращане на пакети, Rx=разрешено приемане на пакети, Dis=портът е забранен;
- **Link** – показва наличието на връзка: Up=има връзка, Down=няма връзка
- **100Mb/s** – скоростта на преноса на данни: Yes=100Mb/s, No=10Mb/s
- **Full Duplex**: Yes=Full, No=Half;
- **Link Quality** – дава оценка на качеството на връзката на този порт. Параметърът е в относителни единици, като 0=максимално качество, а 15 – минимално качество на връзката



Порт 8 е физически разположен до захранващия куплунг на SS8P.



Поставянето на порт в режим Mode=Dis води до логическото му „изключване“ от мрежата. Това обаче не води до промяна на информацията в полето „Link“, т.е. ако на порта има свързан кабел с работещо отсречно устройство, то той ще се индицира като „Up“.



Когато на даден порт няма връзка (Link=Down) не се показват параметрите му и те са заменени със знака „-“.

Кликването в полето с номера на порта води до зареждане на страницата с настройките на избрания порт. Следните параметри са достъпни за конфигуриране в тази страница (някои от тях са директно свързани с показваните в „Port Status“ данни:

- **Enable option:** Tx/Rx = нормална двупосочна работа на порта, Tx = само изпращане на фреймове (forwarding), Rx = само приемане на фреймове, Disable = блокиране на трафика от порта (забрана на порта)
- **Speed, Duplex, Half Duplex Backpressure**

- **Mac Learning:** дава възможност за забрана на „научаването“ на MAC адреси от този порт.
- **Port Priority for Ingress:** квалифициране на ingress трафика на порта като трафик с нисък или висок приоритет.
- **802.1p classification for ingress:** определя дали да се прилага прагът 802.1p (дефинира се „Global Settings“) за определяне на приоритета на трафика.
- **DiffServ classification for ingress:** аналогично, но по отношение на DiffServ полето и стойностите дефинирани в „Global Settings“.

Port 1 Configuration

Enable Option	Tx/Fx
Speed	100Mb/s
Duplex	Full
Half Duplex Backpressure	Enable
MAC learning	Enable
Port Priority for ingress	Low
802.1p classification for ingress	Disable
DiffServ classification for ingress	Disable

Note: Changes take effect after [restart](#) of the switch

## 7.2. Глобални настройки („Global Settings“)

Параметрите от това меню са разделени на две групи и определят общи настройки за целия *SS8P*.

Групата „General“ съдържа някои общи настройки, които не се нуждаят от допълнително разяснение.

Групата „Priority“ съдържа:

- **Priority queues weight** – определя съотношението между трафика с висок към нисък приоритет, което *SS8P* трябва да поддържа: 16:1, 8:1, 4:1, High First (винаги обработва първо високоприоритетния трафик – фреймове с нисък приоритет могат да бъдат блокирани)
- **802.1p high priority threshold** – фреймове от портове, на които е разрешено маркиране на трафика по 802.1p, и които съдържат 802.1p поле със стойност по-голяма от този праг се класифицират с висок приоритет
- **High priority for DiffServ[A],[B]** – с тези две полета се задават DiffServ стойности, които определят трафика, който ги носи като висок приоритет. Двете стойности са независими
- **High priority for IP address/mask [A],[B]** – Определяне на две мрежи (IP/MASK), от които фреймовете ще се квалифицират с висок приоритет

Global Switch Configuration

**General**

Bad packets

Transmit flow control

Receive flow control

Broadcast drop mode

Aging time out

Aging

Tx IPG compensation

LED mode

**Priority related**

Priority queues weight

802.1p high priority threshold

High priority for DiffServ AF,EF and NetworkControl

High priority for DiffServ[A]

High priority for DiffServ[B]

High priority for IP address/mask [A]

IP [A]

Mask [A]

High priority for IP address/mask [B]

IP [B]

Mask [B]

Note: All changes take effect after [restart](#) of the switch

### 7.3. Порт и таг-базирани VLAN („VLAN“)

В това меню се съдържат няколко глобални VLAN настройки, както и таблицата с принадлежности на портовете към различни VLAN групи и индивидуалните настройки на портовете (по отношение на VLAN).



*SS&P не разполага с индивидуални таблици за принадлежност за порт-базиран и таг-базиран VLAN. Таблицата е валидна и за двата типа групиране в зависимост от конкретната конфигурация. Поради това е желателно VLAN да се използва без да се смесват двата типа правила.*

В „Global Control“ са достъпни:

- **VLAN mode** – Глобално разрешаване/забраняване на VLAN обработката (порт- и таг- базирана).
- **802.1q tag aware VLAN** – определя дали да се обработва 802.1q информацията или да се прилагат единствено порт-базирани правила.
- **Ingress is tagged to another VLAN Group** – определя дали да се допускат ingress фреймове, които са тагнати с ID, което се различава от зададеното чрез параметъра PVID за порта, на който пристигат.
- **VLAN tag admit** – дава възможност за „drop“ на нетагнати пакети

Таблицата „VLAN membership table“ определя следното:

- VLANID (VID) на всяка от наличните 9 групи (from A to I) – стойността е всеки валиден таг (0 ... 4095)



- Кои портове (1...8 and C) принадлежат към всяка група и така определяйки към кои портове може да се препраща трафик от дадена група и към коя група се присъединява трафик, носещ даден VID.

### Port and tag based VLAN Configuration

**Global control**

VLAN mode: Disable

802.1q tag aware VLAN: Enable

Ingress is tagged to another VLAN Group: Pass

VLAN tag admit: All

**VLAN membership map and VIDs**

VLAN Groups and VIDs	Port Membership								
	1	2	3	4	5	6	7	8	C
Vlan A <span style="border: 1px solid black; padding: 2px;">0</span>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Vlan B <span style="border: 1px solid black; padding: 2px;">1</span>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Vlan C <span style="border: 1px solid black; padding: 2px;">2</span>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Vlan D <span style="border: 1px solid black; padding: 2px;">3</span>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Vlan E <span style="border: 1px solid black; padding: 2px;">4</span>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Vlan F <span style="border: 1px solid black; padding: 2px;">5</span>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Vlan G <span style="border: 1px solid black; padding: 2px;">6</span>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Vlan H <span style="border: 1px solid black; padding: 2px;">7</span>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Vlan I <span style="border: 1px solid black; padding: 2px;">8</span>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

**802.1q Control Per Port Configuration**

	PVID	Tag Mode	NULL VID Replace	Non PVID Packets Drop
Port 1	<span style="border: 1px solid black; padding: 2px;">A</span>	<span style="border: 1px solid black; padding: 2px;">No change</span>	<input type="checkbox"/>	<input type="checkbox"/>
Port 2	<span style="border: 1px solid black; padding: 2px;">B</span>	<span style="border: 1px solid black; padding: 2px;">No change</span>	<input type="checkbox"/>	<input type="checkbox"/>
Port 3	<span style="border: 1px solid black; padding: 2px;">C</span>	<span style="border: 1px solid black; padding: 2px;">No change</span>	<input type="checkbox"/>	<input type="checkbox"/>
Port 4	<span style="border: 1px solid black; padding: 2px;">D</span>	<span style="border: 1px solid black; padding: 2px;">No change</span>	<input type="checkbox"/>	<input type="checkbox"/>
Port 5	<span style="border: 1px solid black; padding: 2px;">E</span>	<span style="border: 1px solid black; padding: 2px;">No change</span>	<input type="checkbox"/>	<input type="checkbox"/>
Port 6	<span style="border: 1px solid black; padding: 2px;">F</span>	<span style="border: 1px solid black; padding: 2px;">No change</span>	<input type="checkbox"/>	<input type="checkbox"/>
Port 7	<span style="border: 1px solid black; padding: 2px;">G</span>	<span style="border: 1px solid black; padding: 2px;">No change</span>	<input type="checkbox"/>	<input type="checkbox"/>
Port 8	<span style="border: 1px solid black; padding: 2px;">H</span>	<span style="border: 1px solid black; padding: 2px;">No change</span>	<input type="checkbox"/>	<input type="checkbox"/>
Port C	<span style="border: 1px solid black; padding: 2px;">I</span>	<span style="border: 1px solid black; padding: 2px;">No change</span>	<input type="checkbox"/>	<input type="checkbox"/>

Note: Changes take effect after [restart](#) of the switch

Submit

В „802.1q Control Per Port Config” се задават индивидуалните настройки на портовете по отношение на VLAN:

- ✓ **PVID** – определя към коя VLAN група ще се присъединява всеки нетагнат ingress фрейм от порта. Също така определя и тага-ID (зададен на индексиранията VLAN група), с който ще бъдат тагвани фреймовете, получени от този порт и изходящи от тагнат порт.
- ✓ **Tag Mode** – определя как да се обработват egress фреймовете от порта: No change = без да се променят, Tag = тагват се с ID-то на порта източник (source port’s tag) ако са нетагнати и не променят ако вече са тагнати, Untag = премахва таговете от фреймовете, Tag+Replace = тагват се ID-то на порта източник независимо дали фрейма е тагнат/нетагнат.
- ✓ **NULL VID Replace** – определя дали да се подменя нулевия VLAN таг (VID=0), който по принцип има по-специално предназначение

- ✓ **NonPVID Packets Drop** – с тази опция се определя дали *SS8P* ще пропуска ingress фреймове, които са тагнати с ID, различно от това, което се индексира от PVID.



Портът, отбелязан с "C" е специален порт на *SS8P* който не е достъпен.

За детайлно описание на VLAN поддръжката и нейното използване се обърнете към раздел 8.

#### 7.4. Търсене в MAC таблицата („MAC Search“)

Чрез *PicoIP* е възможен достъп до вътрешната MAC таблица на *SS8P*, където може да се провери дали даден MAC адрес е получен от суитча и от кой порт.

За стартиране на процеса на търсене трябва да се въведе валиден MAC адрес – 12 HEX символа и да се стартира търсенето със „Search“ бутона.

Search for entry in switch's MAC table

MAC address  Search...

MAC address must be 12 characters, e.g. 0004235ADD4F

Ако въведеният адрес е намерен ще се изведе резултат от вида:

MAC address search results

Port (1..8)	Age (0..3)	MAC address
01	02	0040F44267EB

Тук се съдържа информация за порта, на който е получен въпросният MAC адрес и стойността на вътрешния таймер за „остаряване“ (age) на записа. Ако търсеният адрес не е намерен таблицата съдържа празни клетки.



Индексирането на MAC таблицата става само по част от битовете на въведения MAC адрес. За това е възможно при търсене на един адрес, в резултатите да фигурира друг MAC адрес. *SS8P* има специална таблица за съхраняване на такъв тип „колизионни“ адреси, но за съжаление достъпът до нея не е възможен.

#### 7.5. Съхраняване на конфигурацията на *SS8P* във файл („Save Config“)

С тази команди се дава възможност на потребителя да запази цялата текуща конфигурация на *SS8P* в бинарен файл. В последствие този файл може директно да бъде зареден в *SS8P*.

#### 7.6. Зареждане на конфигурацията на *SS8P* от файл („Load Config“)

С тази команди се дава възможност на потребителя да зареди в *SS8P* готова конфигурация от бинарен файл.

## 7.7. Зареждане на фабрични настройки в *SS8P* („Default“)

Избирането на това меню води до зареждане в *SS8P* на фабричната му конфигурация, която го превръща в обикновен суитч без VLAN функции. Преди реалното изпълнение на командата се изисква потвърждение от потребителя.

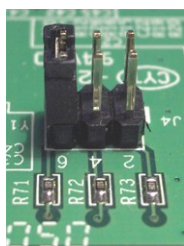
## 7.8. Рестартиране на *SS8P* („Restart“)

Всички направени промени в конфигурацията на *SS8P* се възприемат след рестартирането му. За целта трябва да се потвърди командата.

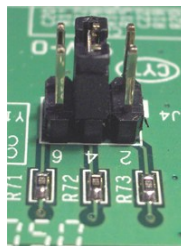
## 7.9. Параметри на *SS8P* , достъпни за конфигуриране с джъмperi

В *SS8P* са предвидени три допълнителни опции за конфигуриране, като тяхното задаване става посредством джъмperi, разположени на платката. Всяка промяна на тези опции изисква рестартиране на *SS8P* (т.е. промените в джъмперите не се възприемат непосредствено).

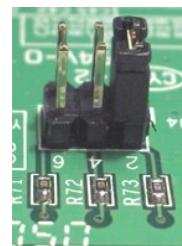
### Broadcast storming



### Port trunking



### Max frame size 1552 bytes



### 7.9.1 „Broadcast storming“ или контрол на „broadcast“ трафика

Добре известно е, че „broadcast“ фреймовете в Ethernet мрежите са с MAC адрес на получателя FF:FF:FF:FF:FF:FF и те се препращат автоматично към всички портове на комутатора, т.е. за тях switch-а работи като „hub“. Поради тази причина, при големи и несегментирани мрежи, този трафик може да нараства лавинообразно и може да влоши работоспособността на цялата мрежа и да претовари мрежовото оборудване.

За предотвратяване на този проблем в *SS8P* е заложена специална функция - „Broadcast Storming“ и тя се избира с поставянето на съответния джъмпер. Джъмперът е фабрично поставен, т.е. функцията е включена по подразбиране.

Същността на функцията се състои в следното – при получаване на даден порт на 64 последователни пакета към адрес FF:FF:FF:FF:FF:FF всички следващи „broadcast“ пакети от този порт биват игнорирани (филтрирани). Това филтриране продължава около 800ms и след това „broadcast“ фреймовете продължават да се обработват нормално (до следващите 64 последователно фрейма). Всеки „multicast“ или „unicast“ пакет също автоматично прекратява този интервал и възстановява нормалната работа.

### 7.9.2 „Port trunking“

Тази функция позволява логическото обединяване на два порта на *SS8P* да функционират като един общ с двойно по-висока скорост на предаване на данните – 200Mb/s, като се използва балансиращ механизъм между портовете. По подразбиране трънк портовете са 1 и 2.

Ако на някой от портовете от трънка е присвоен висок приоритет, то и целият трънк получава такъв приоритет.

За да се използва тази функция е необходимо два *SS8P*, пуснати в трънк режим.



*В ситуация, когато SS8P е в трънк режим и също така се използва VLAN възможно е да възникне ситуация при която пакет се изпраща към трънка, но единият от портовете участници в трънка не от същия VLAN група, от която идва пакета. В такава ситуация VLAN функцията има по-висок приоритет от трънкването и пакета няма да бъде изпратен през порта от трънка.*

### **7.9.3 „Max frame size 1552 bytes“**

По подразбиране *SS8P* обработва пакети с големина до 1536 байта. Поставянето на джъмпера на тази опция води до увеличаване на големината на пропусканите пакети на 1552 байта.

## 8. Решаване на конкретни VLAN задачи с SS8P

Тъй-като VLAN поддръжката на SS8P се различава от стандартната имплементация при скъпите и управляеми суитчове, тук е представено кратко разяснение по отношение третирането на трафика от суитча при различни ситуации.

Както се вижда от таблицата с принадлежностите на портовете към VLAN групите са налице до 9 VLAN групи: от VLANA до VLANI. Всяка група има присвоен VID (0...4095). Нека видим как суитча обработва фреймовете в различни ситуации (режимът „VLAN mode” е разрешен):

1. **Порт получава нетагнат фрейм.** SS8P определя принадлежността на фрейма към една от 9-те VLAN групи според зададения на този порт PVID. Фабричните стойности на PVID са такива, че всеки порт сочи към съответната VLAN група: порт1 към А, порт2 към В и т.н. След определянето на групата, към която принадлежи фрейма се прилага таблицата с принадлежностите (отметките) на портовете към конкретната група: фрейма може да бъде препратен само към порт, който принадлежи на групата (има отметка). Следва отчитане на зададения на изходящия порт „Tag Mode” режим – ако той е конфигуриран да тагва, то фреймът ще излезе от него тагнат с ID-то на VLAN групата към която сочи PVID на порта източник. С други думи при тагването е важен индексът на порта източник, а не този от който „излиза” фрейма.
2. **Порт получава тагнат фрейм.** При тази ситуация SS8P определя принадлежността на фрейма според тага, който носи, а не според порта, от който идва. Естествено ID-то трябва да е зададено на една от VLAN групите. От тук нататък обработката на фрейма протича по аналогичен начин, както в предния случай.



*Задаването на едни и същи PVID на различни портове е напълно допустимо. По този начин трафика от няколко порта се индексира към една VLAN група. Това се използва предимно при таг-базираните конфигурации, когато даден VLAN трябва да се разпределя към няколко порта. При порт-базираните конфигурации обикновено се ползват стандартните стойности на PVID.*



*Не е допустимо задаването на един и същи VLAN ID на различни групи.*



*При използване на SS8P за VLAN-базирано разделяне на трафика трябва да се има предвид, че независимо от възможността да се обособят няколко логически суитча, те ползват обща MAC таблица. Следователно директно свързване на портове от логическите суитчове е недопустимо – това е равносилно на „loop”. Самите VLAN също използват обща MAC таблица.*



*SS8P е основно предназначен за крайни точки в мрежата, а не за “backbone” суитч.*

За онагледяване следват няколко конкретни примера за решаване на различни ситуации

### 8.1. Порт-базиран VLAN: “всички портове виждат един, без да се виждат по между си”

Тази конфигурация има много широко приложение в градските LAN мрежи, тъй-като решава въпросът с неконтролируемият трафик между самите клиенти в нея. Построяването на цяла мрежа чрез конфигурирани по тази схема SS8P дава възможност клиентите да бъдат изолирани един от друг, като имат единствено връзка към сървъра. Това подобрява работата на мрежата и по отношение на

broadcast трафика. На практика мрежата се превръща в дървовидна структура с връх, свързан към сървъра на доставчика.

VLAN mode

802.1q tag aware VLAN

Ingress is tagged to another VLAN Group

VLAN tag admit

VLAN Groups and VIDs	Port Membership								
	1	2	3	4	5	6	7	8	C
Vlan A	0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Vlan B	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Vlan C	2	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Vlan D	3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Vlan E	4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Vlan F	5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Vlan G	6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Vlan H	7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Vlan I	8	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

	PVID	Tag Mode	NULL VID Replace	Non PVID Packets Drop
Port 1	A	No change	<input type="checkbox"/>	<input type="checkbox"/>
Port 2	B	No change	<input type="checkbox"/>	<input type="checkbox"/>
Port 3	C	No change	<input type="checkbox"/>	<input type="checkbox"/>
Port 4	D	No change	<input type="checkbox"/>	<input type="checkbox"/>
Port 5	E	No change	<input type="checkbox"/>	<input type="checkbox"/>
Port 6	F	No change	<input type="checkbox"/>	<input type="checkbox"/>
Port 7	G	No change	<input type="checkbox"/>	<input type="checkbox"/>
Port 8	H	No change	<input type="checkbox"/>	<input type="checkbox"/>
Port C	A	No change	<input type="checkbox"/>	<input type="checkbox"/>

На фигурите е показана необходимата конфигурация в менюто VLAN за решаване на задачата. “Сървърният” порт е с номер 8. Във вид на готов бинарен файл можете да я изтеглите и в последствие заредите в *SS8P* от тук:

[http://lan.neomontana-bg.com/bin/tic\\_vlan.bin](http://lan.neomontana-bg.com/bin/tic_vlan.bin)

Нека проследим как на практика *SS8P* третира трафика. Ако на порт 1 се получи фрейм, то поради това, че PVID=A за този порт, то въпросният фрейм се отнася към VLAN група A. Според отметките в тази група фреймът може да бъде насочен единствено към порт 8 (и порт C, който е със специално предназначение). С други думи клиентът, свързан към порт 1 може да комуникира единствено с порт 8. Ако порт 8 е свързан към следващия конфигуриран по този начин суитч на някои от неговите „клиентски“ портове, то автоматично клиентът от първия суитч не може да комуникира и с клиентите от следващия ... и така единствената му възможна връзка остава към сървъра (който естествено трябва да бъде свързан на порт 8 на последния суитч).

По аналогичен начин се вижда, че и клиентите от портове 2-7 също могат да комуникират само с порт 8. От друга страна фреймовете, постъпващи на порт 8, могат да излязат към всеки един от останалите портове – т.е. сървърът има достъп до всички клиенти.

## 8.2. Порт-базиран VLAN: Разделяне на *SS8P* на два логически 4—портови суитча

Тази конфигурация също добре онагледява възможностите на порт-базирания VLAN в *SS8P*.

Прилагайки разсъжденията от предходния пример лесно се вижда, че портове 1-4 и портове 5-8 са обособени в две отделни групи, в които могат да си комуникират свободно, но не и да излизат извън рамките на групата.

С други думи се получава логическо разделяне на два 4-портови суитча! Важно е да се отбележи, че „двата“ суитча ползват една и съща MAC таблица – следователно е абсолютно недопустимо да има връзка между тях!

Във вид на готов бинарен файл можете да изтеглите конфигурацията и в последствие заредите в *SS8P* от тук:

[http://lan.neomontana-bg.com/bin/tic\\_vlan2.bin](http://lan.neomontana-bg.com/bin/tic_vlan2.bin)

VLAN Groups and VIDs	Port Membership								
	1	2	3	4	5	6	7	8	C
Vlan A 0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Vlan B 1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Vlan C 2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Vlan D 3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Vlan E 4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Vlan F 5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Vlan G 6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Vlan H 7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Vlan I 8	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

### 8.3. Таг-базиран VLAN: Отделяне на до 802.1q трафик към конкретни портове без tag/untag

Това е една класическа конфигурация за таг-базиран VLAN – разполагаме с до 7+2 тагнати VLAN-а, които искаме да отделим към отделни портове (респ. клиенти/мрежи).

VLAN mode

802.1q tag aware VLAN

Ingress is tagged to another VLAN Group

VLAN tag admit

VLAN Groups and VIDs	Port Membership								
	1	2	3	4	5	6	7	8	C
Vlan A 100	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Vlan B 200	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Vlan C 300	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Vlan D 400	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Vlan E 500	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Vlan F 600	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Vlan G 700	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Vlan H 800	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Vlan I 900	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

На фигурата е показана конфигурацията, в която на порт 1 постъпва групата с 7+2 VLAN-а (ID=100,200,300,400,500,600,700,800,900), които трябва да бъдат отделени и изведени на съответните портове (1,2,3,4,5,6,7). Тъй-като допустимият брой VLAN е 9, а портовете с 7 (без входния) то последните два с ID=800,900 са изведени през портове 6 и 7. Във вид на готов бинарен файл можете да изтеглите конфигурацията и в последствие заредите в *SS8P* от тук:

[http://lan.neomontana-bg.com/bin/tic\\_vlan3.bin](http://lan.neomontana-bg.com/bin/tic_vlan3.bin)

Нека проследим в детайли как *SS8P* обработва трафика. Ако на порт 1 постъпи трафик с ID=100, то *SS8P* го отнася към VLANA, тъй-като неговият VID=100. Според отметките на VLANA – този трафик може да бъде пренасочен единствено към порт 2. Тъй-като портовете са в режим „Tag Mode=No change“, то трафикът ще „излезе“ от тях без промени – т.е. от порт 2 ще излезе тагнат с ID=100. Аналогично ще бъде третирането и на ID=200 – към порт 3 ..... до ID=700 – към порт 7.

В обратна посока – ако например на порт 7 постъпи трафик с таг ID=700, то той пак по същите причини, ще бъде отнесен към VLAN G и следователно ще може да „излезе“ единствено през порт 1.

Чрез промяна на отметките може да се направи произволен набор от VLAN-и да излиза от даден порт; например от порт 2 да излизат не само ID=200, но и например 500 и 600.



Какво ще се получи при тази конфигурация, ако на някой от портовете постъпи нетагнат трафик? *SS8P* ще класифицира този трафик според PVID на порта източник и след това отново ще са валидни отметките от таблицата. Например: при порт 7 като източник (PVID=G) – трафикът ще може да излезе единствено през порт 1 ... Ако обработката на нетагнати пакети е нежелателно може да се използва опцията „VLAN tag adim = Only tagged“ - тогава *SS8P* просто ще игнорира нетагнати пакети.



Друга интересна ситуация е когато някой от клиентите, например на порт 2 (който би трябвало да работи с ID=100), се опита да „излезе“ през суитча, но с чужд таг – например ID=200. В общият случай, ако спазваме логиката на класификация според ID-то – то клиентът през порт 2 и с ID=200 би трябвало да може да комуникира спокойно с портове 1 и порт 3 – т.е. да „влезе“ във VLAN 200. Проблемът е, че този клиент никога няма да получи входящ трафик в този VLAN, тъй-като той не членува във VLANB; но въпреки това може да изпрати пакет във VLAN 200. За да може да се ограничи и тази му възможност трябва да се използва опцията „Ingress is tagged to another VLAN Group = Drop“ - тя блокира трафика от порт 2 с ID=200, тъй-като този порт сам по себе си не е член на VLANB!

#### 8.4. Таг-базиран VLAN: Свързване на untag клиент към 802.1q мрежа

Тази конфигурация показва в голяма цялост силата на допълнителните функции на *SS8P*. Тя илюстрира възможността на *SS8P* да тагва/разтагва трафика и да спести използването на скъпи, управляеми суитчове за тази цел.

Задачата е следната: на порт 1 пристигат до 7 тагнати VLAN-а (100-700). Необходимо е тези VLAN-и да се разпределят към портове 2-8, като паралелно с това от тези портове трафикът да излезе нетагнат и към тях да могат директно да се свържат нетагнати клиенти/мрежи. Във вид на готов бинарен файл можете да изтеглите конфигурацията и в последствие заредите в *SS8P* от тук:

[http://lan.neomontana-bg.com/bin/tic\\_vlan4.bin](http://lan.neomontana-bg.com/bin/tic_vlan4.bin)

По отношение на разделянето на VLAN задачата е подобна на предния пример. Разликата идва от настройките на самите портове: „клиентските“ портове са в режим „Tag mode = Untag“, а входният порт - „Tag mode = Tag“.

	PVID	Tag Mode	NULL VID Replace	Non PVID Packets Drop
Port 1	A	Tag	<input type="checkbox"/>	<input type="checkbox"/>
Port 2	B	Untag	<input type="checkbox"/>	<input type="checkbox"/>
Port 3	C	Untag	<input type="checkbox"/>	<input type="checkbox"/>
Port 4	D	Untag	<input type="checkbox"/>	<input type="checkbox"/>
Port 5	E	Untag	<input type="checkbox"/>	<input type="checkbox"/>
Port 6	F	Untag	<input type="checkbox"/>	<input type="checkbox"/>
Port 7	G	Untag	<input type="checkbox"/>	<input type="checkbox"/>
Port 8	H	Untag	<input type="checkbox"/>	<input type="checkbox"/>
Port C	I	Untag	<input type="checkbox"/>	<input type="checkbox"/>

Значението на тази настройка на портовете е очевидна – клиентските портове трябва да премахнат таговете от трафика; входният порт трябва да тагне нетагнатият клиентски трафик за да може той да „влезе“ в съответния VLAN.

Много важно е да се отбележи, че тагването в порт 1 става с тага на порта източник!!! Тагът на порта източник се определя от стойността на PVID на този порт и след това от стойността на VID за VLAN групата към която сочи PVID. Например, ако на порт 7 пристигне нетагнат клиентски трафик, то според отметките той може да отиде към порт 1, който обаче трябва да го тагне. Тъй-като на порт 7 PVID=G, съответно VID=700 за VLANG: тагването в порт 1 става с ID=700.



При тази конфигурация НЕ е възможно в порт 1 да се „влезе“ в *SS8P* с нетагнат трафик! Причината за това е, че дори и „влизането“ да не е тагнато ... то трафикът, който излиза от порт 1 ВИНАГИ е тагнат (заради „Tag mode = Tag“). Поради тази причина този тип приложение на *SS8P* е удачно да се използва в края на мрежата, непосредствено преди клиента.





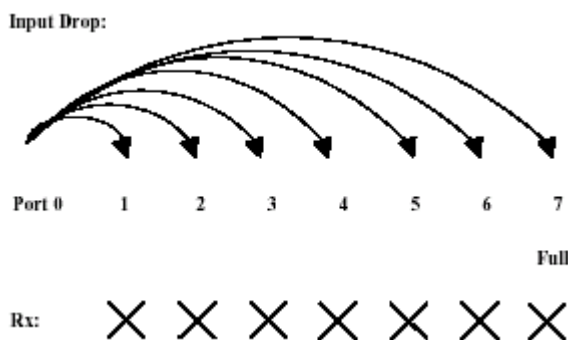
И при тази конфигурация са възможни опити за „прескачане“ на клиенти от един VLAN в друг. Единият от начините да се ограничат такива опити е порт 1 да се постави в режим „Tag Mode = Tag+Replace“ - в този случай порт 1 не само ще тагва нетагнатият трафик от останалите портове, но и ще подмени техните тагове (ако вече са тагнати) с тага сочен от PVID. По този начин от порт 7 например, през порт 1 винаги ще излизе трафик с ID=700 независимо дали клиентът на порт 7 е нетагнат или тагнат с някакъв таг. Друго решение е да се използва опцията на клиентските портове „Non PVID Packets Drop“. Тя води до недопускане в SS&P на тагнат трафик, чиито таг не съпада с тага, който се определя от PVID!

## 9. Параметър "Broadcast Drop Mode"

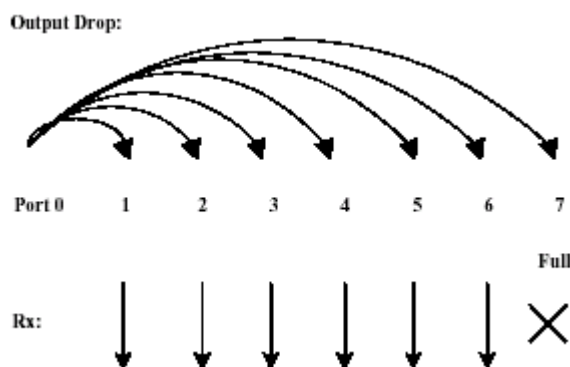
Това е допълнителна функция за управление на broadcast трафика, независимо от "Broadcast Storming". Тя е достъпна от менюто "Global Settings".

Тя също контролира broadcast трафика в случай на претоварени портове. При наличие на "блокирани" от трафик портове и пълен вътрешен буфер, то "broadcast" пакетите също биват игнорирани, като са възможни два начина на работа:

- **Input Drop:** при този режим пакетите се игнорират още на входа на *SS8P* в случай, че буфера на някой от портовете е пълен. Въпреки, че този режим ефективно намалява натоварването на *SS8P*, то "broadcast" пакетите и към свободните портове също биват игнорирани;



- **Output Drop:** в този случай се спират "broadcast" пакетите само към претоварените портове, но към останалите биват препращани.



*Тази опция въздейства по същия начин и върху multicast трафика. При използване на *SS8P* за multicast IPTV тя трябва да бъде поставена в „Output Drop“*