Гигабитови SFP

суитчове

с IGMP Snooping V1/V2/V3

и управление през PicoIP v2

NMGS4P1F-IS

1x1.25G SFP + 4x10/100/1000 RJ-45

NMGS4P2F-IS

2x1.25G SFP + 4x10/100/1000 RJ-45

Ръководство на потребителя

rev. 1.03

10.2022

СЪДЪРЖАНИЕ

1. Версии на документа

Версия	Дата	Кратко описание на въведените промени
1.03	1.10.2022 г.	Промяна в снимката с монтиран кабел на NMGS4P1F-IS
1.02	22.12.2016	Промяна в горната граница на захранващото напрежение – от 24VDC на 18VDC
1.00	12.11.2015	Начална версия на документа

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!

2. Въведение

NMGS4PxF-IS е мрежов комутатор за 10/100/1000 Ethernet със слот/ове за оптичен 1.25G SFP модул специално разработен съгласно нуждите на операторите, изграждащи градски LAN мрежи.

Това, което го отличава от останалите подобни продукти са:

- гарантирания нисък стартов ток и обща консумация на енергия;
- Green Ethernet с изключително ниска консумация: NMGS4P2F-IS - 150mA@12V (с 2бр. SFP модули на 20km и 4x1G на медните портове); консумация без SFP модули - макс. 70mA@12V
- широк диапазон на захранващо напрежение: от 5 до 18VDC.
- Стабилна работа при ТОКОВИ УДАРИ, благодарение на вградения ХАРДУЕРЕН МОНИТОРИНГ за пропадане на захранващото напрежение, който осигурява винаги пълен рестарт на процесора в такива ситуации
- Вградена хардуерна поддръжка на IGMP Snooping V1/V2/V3 - прави продукта изключително подходящ за Mutlcast IPTV системи
- Възможност за управление и конфигуриране през ***PicoIPv2***
- 2K MAC таблица
- Размери: 140x105x26mm
- Окомплектовка: без захранващ адаптер

Без наличието на управляващ ***PicoIPv2*** модул, суитчът може да се използва като обикновен суитч в 10/100/1000 LAN мрежи. Свързването му към ***PicoIPv2*** позволява да се получи достъп до допълнителните му функции. Когато ***PicoIPv2*** остава постоянно свързан към ***NMGS4PxF-IS*** това превръща двете устройства в управляем суитч (***PicoIPv2*** дава достъпа по IP адрес да конфигурацията на ***NMGS4PxF-IS***).

Възможно е и използването на ***PicoIPv2*** само като „програмиращ“ модул, чрез който да получите достъп до параметрите на ***NMGS4PxF-IS***, но като цяло да няма необходимост от постоянен достъп и възможност за тяхната промяна в последствие. Така, след въвеждане на необходимата конфигурация в ***NMGS4PxF-IS***, се премахва ***PicoIPv2***, а ***NMGS4PxF-IS*** запазва в енергонезависима памет своята конфигурация.

Суитчът не се поддържа от по-старите версии на PicoIP!

3. Основни функции и параметри *NMGS4PxF-IS*

3.1. Уникални функции в *NMGS4PxF-IS*

- ✔ Разширен диапазон на захранване: 5 – 18VDC
- ✔ Вграден активен мониторинг на захранването за защита от „забиване“ в следствие на токови удари

3.2. Други функции

- ✔ GreenEthernet
- ✔ “Изключване“ на портовете, на които няма връзка (PowerDown)
- ✔ 4 порта 10/100/1000Base T/TX Nway (Auto-negotiation) суитч с екранирани RJ-45 конектори;
- ✔ 1 или 2бр. 1.25G SFP слота.
- ✔ Изключително ниска консумация на енергия – оптимално решение за PoE системи;
- ✔ Автоматично „научаване“ на мрежовата топология;
- ✔ Автоматично разпознаване на „Full“/“Half“ дуплекс режим;
- ✔ „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
- ✔ Max frame size: 1552 байта

3.3. Допълнителни функции, достъпни през PicoIPv2

- ✔ Порт-базирано VLAN групиране в 8 групи;
- ✔ 802.1q порт/таг базиран VLAN до 8 групи;
- ✔ Възможност за вмъкване/премахване на 802.1q тагове на всеки порт;
- ✔ Настройваемо време на обновяване на MAC таблицата (Age Timeout)
- ✔ Детайлен статус на портовете: връзка, скорост, FlowControl
- ✔ Листване на MAC таблицата за целия суитч или зададен порт
- ✔ FlowControl активиране/деактвиране за всеки порт
- ✔ IGMP настройки

3.4. Технически параметри

Стандарти

IEEE 802.3 10BASE-T
IEEE 802.3u 100BASE-TX
IEEE 802.3u 1000BASE-T

Брой портове

4 интегрирани порта (10/100/1000Mbps Nway)
1/2 порта SFP за 1.25G оптични модули

Поддръжка на “Flow Control”

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

Индикатори

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

Общ: POWER

Захранване

- Работна стойност на захранването: 5VDC – 18VDC;
- Конектор: Жак (2.1mm) 

Работен температурен обхват: 0°~ 55°

Температура на съхранение: -20°~ 90°

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

4. Свързване на *PicoIPv2* към *NMGS4PxF-IS*

Желателно е захранването на двете устройства да става от един и същи захранващ източник! Свързването да става при изключено захранване на устройствата!

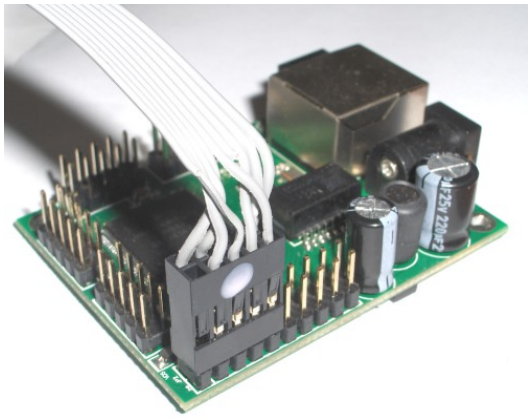
*Във фабричните настройки на PicoIPv2 режимът „Switch Control" (управление на **NMGS4PxF-IS**) е ИЗКЛЮЧЕН! За да получите достъп до параметрите на **NMGS4PxF-IS** трябва да пуснете режима през Web: опцията „Switch Control Mode", която се намира „Setup->Switch Control „.*

PicoIPv2 и ***NMGS4PxF-IS*** 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.

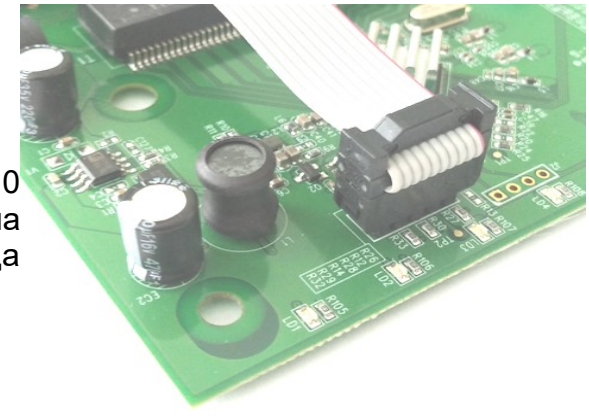
*Тази връзка единствено дава възможност на PicoIPv2 за контрол на **NMGS4PxF-IS**.Тя не осигурява Ethernet линка към **PicoIPv2** – той трябва отделно да се свърже в мрежата чрез патч кабел. Тази връзка също не осигурява захранване на единия или другия модул.*

При необходимост от постоянен "on-line" достъп за управление на ***NMGS4PxF-IS***, ***PicoIPv2*** остава свързан към него постоянно.

В много случай, може да е достатъчна само възможността в ***NMGS4PxF-IS*** да се зареди някаква специфична конфигурация (например VLAN групиране на портовете, с цел създаване на логически сегменти). Тогава ***PicoIPv2*** модулът се използва като програматор и след зареждане на необходимата конфигурация, той се демонтира от ***NMGS4PxF-IS***. С цел лесно зареждане на една и съща конфигурация в много на брой ***NMGS4PxF-IS*** в клиентските приложения, както и във Web сървъра, е предвидена възможност за съхраняване/зареждане на конфигурацията във файл.



1.) Куплунгът от страната на ***PicoIPv2*** е маркиран със сива точка. Той се поставя върху пинове 1-10 от JP2 така, че точката да остане извън платката на устройството.



2.) Другият край на кабела с IDC10 куплунг се поставя на конектора JP1 на ***NMGS4PxF-IS***, така че лентовият кабел да „сочи" към RJ45 куплунзите.

5. Достъп през WEB до параметрите на *NMGS4PxF-IS*

Достъпът до параметрите на ***NMGS4PxF-IS*** е възможен чрез Web браузър и връзка към IP адреса на ***PicoIPv2.***

За достъп до различните параметри на ***NMGS4PxF-IS*** през Web е обособена отделна категория в Web страницата на ***PicoIPv2*** – „Switch Control". Детайлно описание на менютата е поместено в следващия раздел.

*Промяната на който и да е параметър от настройките на **NMGS4PxF-IS** се възприема ВЕДНАГА!!! (за разлика от други модели суитчове).*

Направените промени обаче се съхраняват в енергонезависимата памет на суитча ЕДИНСТВЕНО след изпълнение на командата „Store Config". Тя предизвиква запазване на текущите настройки на суитча и рестартирането му веднага след това.

Ако рестартирате суитча преди изпълнението на тази команда, то в него ще се заредят последните съхранени стойности на параметрите и текущата конфигурация ще се загуби.

5.1. Функция "Smart Configuration Apply"

Това е специално проектирана системна функция на ***PicoIPv2***, предназначена за предпазване от "лошо" конфигуриране на ***NMGS4PxF-IS*** особено, когато към него е свързан и Ethernet линка на ***PicoIPv2***. Такова конфигуриране би могло да прекрати достъпа до ***PicoIPv2*** модула през мрежата и да го направи изцяло недостъпен.

"Smart Configuration Apply" се грижи за това да провери дали след реконфигурирането на ***NMGS4PxF-IS***, връзката до ***PicoIPv2*** се е запазила. Потвърждаването, че има достъп до ***PicoIPv2*** става с достъп през Web до някоя от страниците му или чрез достъп до специално заделен SNMP OID (rtlApply.0). Изпълнението на което и да е от двете деактивира режима.

Ако не се „потвърди" достъпа до ***PicoIPv2*** по един от начините и изтече времето от около 2 минути, ***PicoIPv2*** ще предприеме следните действия:

1) Ако последната изпълнена команда е била зареждане в суитча на готова конфигурация от файл (менюто „From file ...") то тогава в суитча се възстановява фабричната му конфигурация и той се рестартира;
2) Ако последната команда е била някаква настройка от менюто „Global Settings" или „VLAN" то тогава суитчът само ще рестартира (което ще доведе до зареждане на последната съхранена конфигурация) като се разчита, че последната запазена в него конфигурация е с нормален достъп до ***PicoIPv2***.

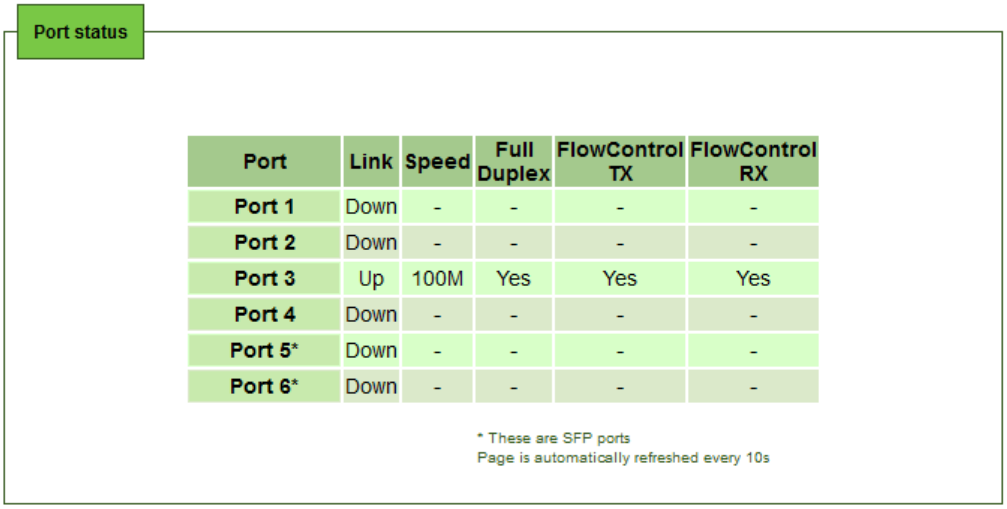
*Задействането на този механизъм временно (до изтичане на 2min или до потвърждаване на настройките по един от описаните начини) преустановява рестартирането на **NMGS4PxF-IS** в следствие на ICMP мониторинг събития. По този начин се предпазва **NMGS4PxF-IS** от рестартиране по време на конфигуриране, което може да доведе до възприемане на непълна конфигурация.*

6. Кратко описание на функциите на *NMGS4PxF-IS*

В този раздел са описани всички налични за настройка функции и параметри на ***NMGS4PxF-IS***. За онагледяване е използван Web интерфейсът на ***PicoIPv2***.

6.1. Статус на портовете („Port Status“)

Страницата показва текущото състояние на всички портове на ***NMGS4PxF-IS***. Тя се презарежда автоматично на всеки 10 секунди.



Страницата предоставя следната информация:

- **Port** – определя номера и името на порта. Портовете могат да се именуват през менюто „Port Labels” на ***PicoIPv2.***
- **Link** – показва наличието на връзка: Up=има връзка, Down=няма връзка
- **Speed** – показва на каква скорост работи порта
- **Full Duplex**: Yes=Full, No=Half;
- **FlowControl Tx/Rx** – показва дали тази функция е активна за порта или не

Порт 1 е първият RJ45 порт от към захранването на суитча.
*Порт 5 и 6 са SFP слотовете. На **NMGS4P1F-IS** е наличен само порт 5.*

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

6.2. Глобални настройки („Global Settings“)

Тук са поместени няколко общи за целия суитч настройки.

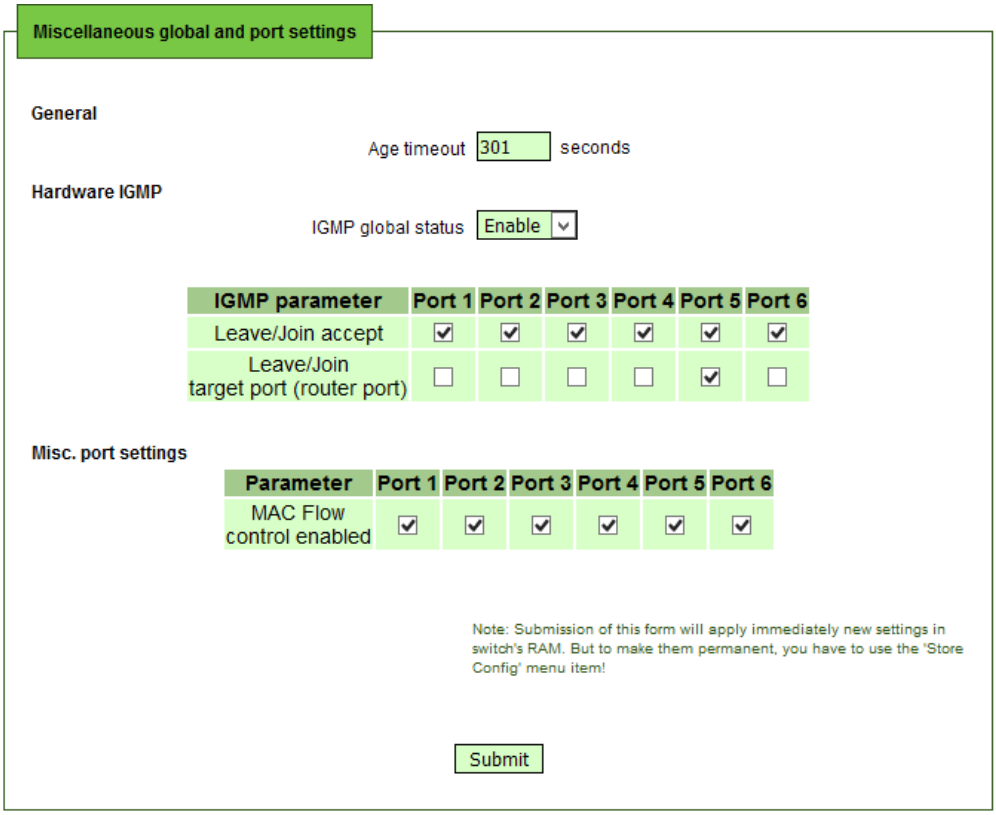
Първата настройка е за „Age Timeout” - времето за „забравяне“ на записан в MAC таблицата адрес, когато той вече не е активен на портовете. Времето е в секунди. Фабричната стойност е 300s (5 минути).

Втората група е за хардуерната IGMP поддръжка на суитча. Съдържа следните параметъра:

- **IGMP Global status** – определя дали IGMP обработката изобщо да се осъществява от суитча или не (изключване на IGMP).
- **Leave/Join accept** – за кои портове е разрешено да получават и обработват IGMP Leave/Join фреймове. Това са обикновенно клиентските портове.

- **Leave/Join target port (router port)** – определя КЪМ кой порт е разрешено да се насочват IGMP Leave/Join фреймовете. Това обикновено е рутерният порт, зад който се намира мултикаст сървъра.

Последната настройка дава възможност да се активира/деактивира FlowControl на вграденият MAC лейър за всеки порт в суитча.



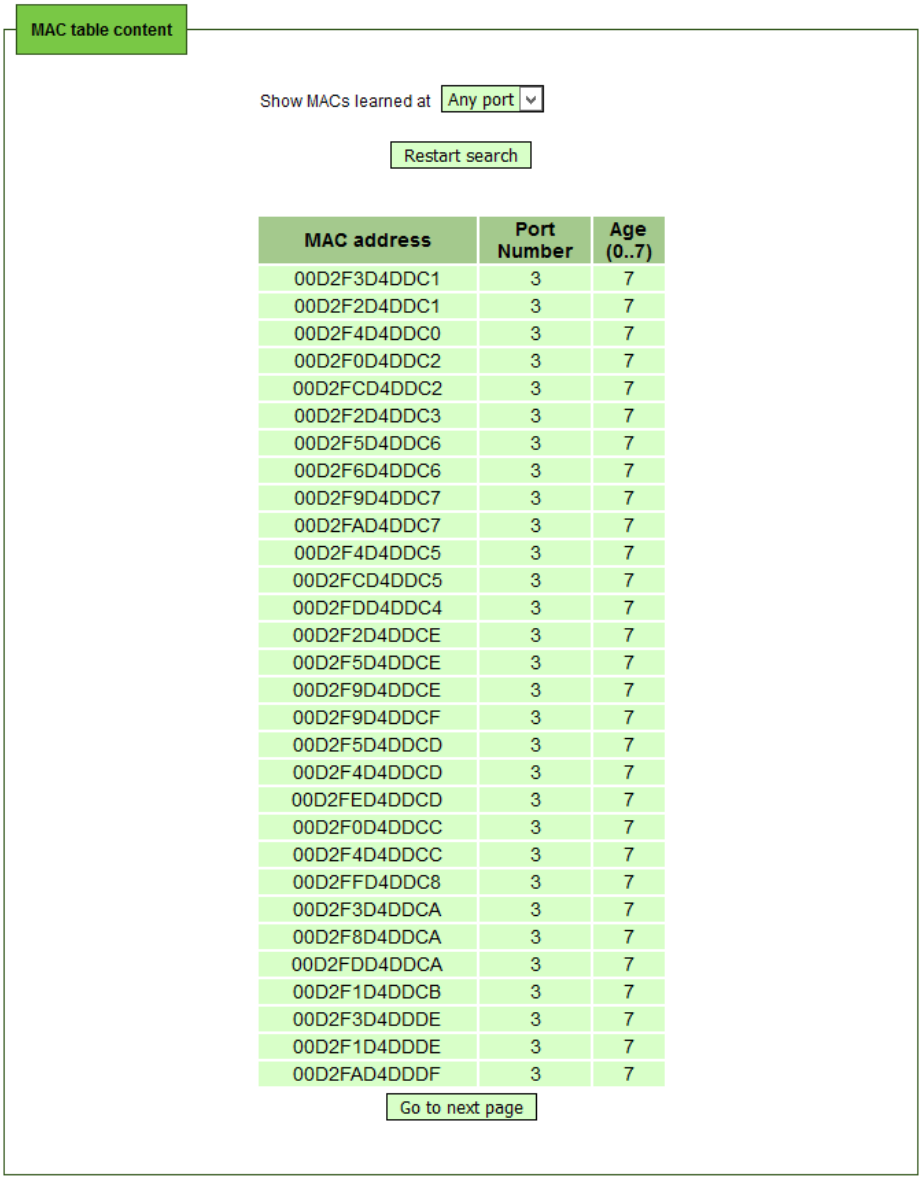
6.3. Достъп до MAC таблицата („MAC List")

Чрез това меню може да се покажат записите в MAC таблицата на суитча.

Можете да филтрирате данните само по адреси, получени на даден порт или да покажете всички записи.

За всеки запис в таблицата се показва адресът, на който порт е обучен и относителното му време (0..7) до премахването му от таблицата.

Когато данните са много, под списъка се появява бутона „Go To Next Page". Странирането е само в посока „напред" - не можете да се върнете в предишна страница (единствено можете да стартирате нов търсене от самото начало с бутона „Restart Search").



6.4. Порт и таг-базирани VLAN („VLAN“)

В това меню се съдържат настройки за 802.1q VLAN, както и за порт-базиран VLAN. Настройките са разделение на три групи/таблици: общи настройки, 802.1q и порт-базирани.

Общите настройки за всеки порт в таблицата „Per port settings for 802.1q and port-based VLAN“ са както следва:

„802.1Q mode“ – общ режим на работа на порта	
Port-base	В този режим портът работи единствено по порт-базираните правила от таблицата „Port-based VLAN Members“. 802.1q е изключена.
Fallback	Когато суитчът получи тагнати фреймове с тагове, които не са описани в таблицата „802.1Q VIDs and egress port settings“ за тях ще се прилагат порт-базираните правила. За останалите 802.1q правилата.
Check	Допуска на порта VID, различни от тези, на които порта е член (т.нар. 'alien' VID). Но не допуска (drop) фреймове с VID, който не е описан в таблицата.

Secure	Допуска ЕДИНСТВЕНО VID, на които порта е член. Всичко останало се филтрира (drop).

„INGRESS pass mode“ – режим на работа на порта относно входящи фреймове	
All	Допускат се всякакъв тип входящи фреймове за порта
Tag only	Допускат се само тагнати фреймове
Untag only	Допускат се само ънтагнати фреймове

„EGRESS pass mode“ – режим на работа на порта относно изходящи фреймове	
All	Разрешено е да „излизат“ от порта всякакви типове фреймове
Tagged only	Само тагнати фреймове могат да „излизат“ от порта

„EGRESS mode for port-based“ – режим на манипулиране на изходящия от порта трафик в порт-базиран режим	
Unmodify	Запазва резултатът от обработката на фрейма (реално дори и нетагнатите фреймове се приравняват към тагнати през „Default VID”)
Untouch	Запазва първоначалната енкапсулация на фрейма, така както е постъпил в суитча.
Untag	Портът е Untagged Port – таговете се премахват от изходящия трафик
Tag	Портът е Tagged Port – винаги се добавя тагове към изходящия трафик. *Важно е да се отбележи, че при този режим таговете, които се поставят на изходящия от порта трафик се „вземат“ от полето „Default VID for untagged” за порта източник.*

„Default VID for untagged“ – стойност на VID по подразбиране (0...4095) за нетагнати фреймове, постъпващи на даден порт.

На практика, чрез това поле, за по нататъшната обработка на фрейма може да се счита, че той е тагнат с тази стойност. Поради това, този VID ще се използва за тагване в последствие от изходящ порт в режим „Tag”или „Unmodify”, както и за проверките в режимите „Secure”, “Check” и т.н.

“Force Default VID” - Указва дали при тагнат входящ трафик на порта да се форсира към „Default VID”, независимо какъв таг носи фрейма.

В следващата таблица „802.1Q VIDs and egress port settings“ са настройките за тагнат режим. Те са без значение за портове в режим „Port-based”.

За да се дефинира VLAN трябва да се постави отметка в 'Enabled', да се зададе тага в полето 'VLAN's ID' и да се укаже EGRESS режима на всеки порт. Режимите са съответно 'Pass', 'Untag', 'Tag' и 'Drop'.

Последната таблица е за порт-базиран режим и определя кой порт с кой може да си комуникира (не забравяйте, че комуникацията е двупосочна и има отметки по редове и по колони). Тези настройки са валидни за портове в режим 'Port-based' или 'Fallback'.

По подразбиране таблицата е с поставени отметки на всички комбинации от двойки портове, с изключение на диагонала (порт към самия себе си).

За конкретни примери с VLAN се обърнете към раздел 7.

Port and tag based VLAN Configuration

Per port settings for 802.1q and port-based VLAN

Port	802.1Q mode *	INGRESS pass mode **	EGRESS pass mode	EGRESS mode for port-based	Default VID for untagged	Force Default VID
Port 1	Port-base	All	All	Untouch	1	☐
Port 2	Port-base	All	All	Untouch	1	☐
Port 3	Port-base	All	All	Untouch	1	☐
Port 4	Port-base	All	All	Untouch	1	☐
Port 5	Port-base	All	All	Untouch	1	☐
Port 6	Port-base	All	All	Untouch	1	☐

* 'Port-base'=Disable 802.1q, use only port-based rules; 'Fallback'=Use port-based rules for undefined VIDs; 'Check'=Allow allen VIDs, drop undefined; 'Secure'=Drop allen and undefined VIDs
** INGRESS pass mode works in both 802.1Q and port-based modes!

802.1Q VIDs and egress port settings (applicable only when 802.1Q mode is 'Check' or 'Secure')

Enabled	VLAN's ID	Port Membership EGRESS rule					
		Port 1	Port 2	Port 3	Port 4	Port 5	Port 6
☐	0	Pass	Pass	Pass	Pass	Pass	Pass
☐	0	Pass	Pass	Pass	Pass	Pass	Pass
☐	0	Pass	Pass	Pass	Pass	Pass	Pass
☐	0	Pass	Pass	Pass	Pass	Pass	Pass
☐	0	Pass	Pass	Pass	Pass	Pass	Pass
☐	0	Pass	Pass	Pass	Pass	Pass	Pass
☐	0	Pass	Pass	Pass	Pass	Pass	Pass
☐	0	Pass	Pass	Pass	Pass	Pass	Pass

Port-based VLAN Members (applicable only when 802.1Q mode is 'Port-based' or 'Fallback')

	Port 1	Port 2	Port 3	Port 4	Port 5	Port 6
Port 1	☐	☑	☑	☑	☑	☑
Port 2	☑	☐	☑	☑	☑	☑
Port 3	☑	☑	☐	☑	☑	☑
Port 4	☑	☑	☑	☐	☑	☑
Port 5	☑	☑	☑	☑	☐	☑
Port 6	☑	☑	☑	☑	☑	☐

Note: Submission of this form will apply immediately new settings in switch's RAM.
But to make them permanent, you have to use the "Store Config" menu item!

Submit

6.5. Запазване на текущата конфигурация в енергонезависимата памет на *NMGS4PxF-IS* („Store Config“)

Както стана вече дума, всяка промяна в настройките на суитча се възприема мигновено. Тя обаче се зарежда единствено в оперативната памет на суитча и при рестартиране би се загубила.

За това след приключване на конфигурирането е **ЗАДЪЛЖИТЕЛНО** чрез това меню да се направи „запис“ на настройките в енергонезависимата му памет. Те ще бъдат заредени от нея при всяко включване/рестартиране на суитча.

6.6. Съхраняване на конфигурация на *NMGS4PxF-IS* във файл („To file ...“)

С тази команди се дава възможност на потребителя да запази цялата текуща конфигурация от енергонезависимата памет на ***NMGS4PxF-IS*** в бинарен файл. В последствие този файл може директно да бъде зареден в ***NMGS4PxF-IS***. Изпълнението на тази команда рестартира суитча!

Преди използването на тази команда изпълнете „Store Config” за да сте сигурни, че в енергонезависимата памет е записана последната направена конфигурация. Ще получите и подсещащо съобщение за това в браузера.

6.7. Зареждане на конфигурацията на *NMGS4PxF-IS* от файл („From file … “)

С тази команди се дава възможност на потребителя да зареди в ***NMGS4PxF-IS*** готова конфигурация от бинарен файл. Изпълнението на тази команда рестартира суитча!

6.8. Зареждане на фабрични настройки в *NMGS4PxF-IS* („Default Config“)

Избирането на това меню води до зареждане в ***NMGS4PxF-IS*** на фабричната му конфигурация, която го превръща в обикновен суитч. Преди реалното изпълнение на командата се изисква потвърждение от потребителя. Изпълнението на тази команда рестартира суитча!

6.9. Рестартиране на *NMGS4PxF-IS* („Reboot“)

Командата рестартира суитча. Ако текущите настройки не сте ги съхранили с „Store Config” суитчът ще презареди настройките, които последно са запазени в енергонезависмата му памет.

7. Решаване на конкретни VLAN задачи с *NMGS4PxF-IS*

Първо ще поясним в каква последователност се прилагат различните настройки при постъпване на фрейм в суитча тъй-като порт и таг-базираният VLAN реално се настройват съвместно.

СТЪПКА 1: Прилага се филтъра „INGRESS pass mode“

СТЪПКА 2: Прилага се „Default VID for untagged“. Ако опцията „Force Default VID“ е включена с този VID се „замества“ тага, който носи фрейма; иначе ако фреймът е тагнат той се запазва.

СТЪПКА 3: Проверява се „802.1Q mode“ за порта. Според стойността има два варианта:

При „802.1Q mode“ = Port-based

СТЪПКА 4: Проверява се таблицата за порт-базиран VLAN. Ако портът получател е разрешен в таблицата фреймът се насочва към него. В противен случай той се „изхвърля“ от суитча.

СТЪПКА 5: На порта получател се прилага настройката от „EGRESS mode for port-based“ и се изпраща през порта. Ако настройката е 'Tag' или 'Unmodify' то изходящият фрейм бива тагнат с VID на порта източник (в случая порта източник е нетагнат и за това се ползва неговото 'Default VID').

При „802.1Q mode“ = Fallback, Check *или Secure*

СТЪПКА 4: Проверява се дали фреймът носи VID, който е описан в таблицата „802.1Q VIDs“. Ако го няма дефиниран: в режим „Fallback” се отива не стъпка 4 от порт-базираната последователност от действия (т.е. се преминава в порт-базиран режим), а за другите два режима – фреймът се „изхвърля“. Ако е дефиниран се отива на следващата стъпка

СТЪПКА 5: Проверява се портът, получател на този фрейм, дали членува във VLAN-а с носения VID. Ако не членува и режимът е Secure – фреймът се „изхвърля“. Иначе се продължава на следващата проверка

СТЪПКА 6: За порта получател се прилага настройката му за намерения VLAN „Port Membership EGRESS rule“ от таблицата „802.1Q VIDs“ и фреймът напуска суитча ако е в режими „Pass”, “Tag”, “Untag”. В режим „drop” фреймът се „изхвърля“.

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

7.1. 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 *NMGS4PxF-IS* 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 и не дава възможност на клиентите да „напълнят“ мрежата с локален трафик и така да влошат достъпа на останалите клиенти до услугите на доставчика.

На практика мрежата се превръща в дървовидна структура с връх, свързан към сървъра на доставчика и комуникацията е разрешена само от „листата“ към върха, но не и между тях.

Per port settings for 802.1q and port-based VLAN

802.1Q mode *	INGRESS pass mode **	EGRESS pass mode	EGRESS mode for port-based	Default VID for untagged	Force Default VID
Port-base	All	All	Untouch	1	☐

Port-based VLAN Members (applicable only when 802.1Q mode is 'Port-based' or 'Fallback')

	Port 1	Port 2	Port 3	Port 4	Port 5	Port 6
Port 1	☐	☐	☐	☐	☑	☐
Port 2	☐	☐	☐	☐	☑	☐
Port 3	☐	☐	☐	☐	☑	☐
Port 4	☐	☐	☐	☐	☑	☐
Port 5	☑	☑	☑	☑	☐	☑
Port 6	☐	☐	☐	☐	☑	☐

На фигурите е показана необходимата конфигурация в менюто VLAN за решаване на задачата. “**Сървърният” порт е с номер 5 (SFP порта)**. Всички портове трябва да са в режим „Port Base” и в таблицата с отметките да се укаже, че всички могат да комуникират само с Port 5 (и в двете посоки).

7.2. Порт-базиран VLAN: Разделяне на *NMGS4PxF-IS* на два логически портови суитча

Тази конфигурация също добре онагледява възможностите на порт-базирания VLAN в ***NMGS4PxF-IS***.

Прилагайки разсъжденията от предходния пример лесно се вижда, че портове 1-3 и портове 4-6 са обособени в две отделни групи, в които могат да си комуникират свободно, но не и да излизат извън рамките на групата.

Port-based VLAN Members (applicable only when 802.1Q mode is 'Port-based' or 'Fallback')

	Port 1	Port 2	Port 3	Port 4	Port 5	Port 6
Port 1	☐	☑	☑	☐	☐	☐
Port 2	☑	☐	☑	☐	☐	☐
Port 3	☑	☑	☐	☐	☐	☐
Port 4	☐	☐	☐	☐	☑	☑
Port 5	☐	☐	☐	☑	☐	☑
Port 6	☐	☐	☐	☑	☑	☐

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 патч връзка между тях!

7.3. Таг-базиран VLAN: Свързване на untag клиенти към 802.1q мрежа

Тази конфигурация показва най-пълно силата на допълнителните функции на ***NMGS4PxF-IS***. Тя илюстрира възможността на ***NMGS4PxF-IS*** да тагва/разтагва трафика и да спести използването на скъпи, управляеми суитчове за тази цел.

Задачата е следната: на порт 6 на ***NMGS4P2F-IS*** пристигат 5бр. тагнати VLAN-а (100,200,300,400,500). Целта е тези VLAN-и да се разпределят към портове 1-5, като

паралелно с това от тези портове трафикът да излезе нетагнат и към тях да могат директно да се свържат нетагнати клиенти/мрежи.

Едно от възможните решения е показано на следващата илюстрация:

Per port settings for 802.1q and port-based VLAN

Port	802.1Q mode *	INGRESS pass mode **	EGRESS pass mode	EGRESS mode for port-based	Default VID for untagged	Force Default VID
Port 1	Secure	All	All	Untouch	100	☐
Port 2	Secure	All	All	Untouch	200	☐
Port 3	Secure	All	All	Untouch	300	☐
Port 4	Secure	All	All	Untouch	400	☐
Port 5	Secure	All	All	Untouch	500	☐
Port 6	Secure	All	All	Untouch	1	☐

* 'Port-base'=Disable 802.1q, use only port-based rules; 'Fallback'=Use port-based rules for undefined VIDs; 'Check'=Allow alien VIDs, drop undefined; 'Secure'=Drop alien and undefined VIDs

** INGRESS pass mode works in both 802.1Q and port-based modes!

802.1Q VIDs and egress port settings (applicable only when 802.1Q mode is 'Check' or 'Secure')

Enabled	VLAN's ID	Port Membership EGRESS rule					
		Port 1	Port 2	Port 3	Port 4	Port 5	Port 6
☑	100	Untag	Drop	Drop	Drop	Drop	Tag
☑	200	Drop	Untag	Drop	Drop	Drop	Tag
☑	300	Drop	Drop	Untag	Drop	Drop	Tag
☑	400	Drop	Drop	Drop	Untag	Drop	Tag
☑	500	Drop	Drop	Drop	Drop	Untag	Tag
☐	0	Pass	Pass	Pass	Pass	Pass	Pass
☐	0	Pass	Pass	Pass	Pass	Pass	Pass
☐	0	Pass	Pass	Pass	Pass	Pass	Pass

Всички портове са поставени в режим 'Secure' за да не се допуска достъп от неописани VLAN-и. **Много важно е задаването на „Default VID for untaged" за всеки от клиентските портове – по този начин определяме нетагнатият трафик, постъпващ на портове от 1 до 5 какъв VID да му се присвои.** В таблицата за 802.1Q се описани въпросните VID и съответния достъп на портовете: за порт 6 всички настройки са в „Tag" режим (за да излиза от него тагнат трафика от клиентските портове към сървъра), а за клиентските портове в даден VLAN е зададен режим „Untag" за да се премахне тага на входящия от порт 6 трафик и да се изпрати към клиентския порт без таг. Естествено всчки портове в чужди VLAN са в режим „Drop" за да не може клиент от порт 2 да „вижда" VLAN с VID=300.

Може да се добавят и други опции, например за клиентските портове да се пусне „INGRESS pass mode=Untag only" и така да им се забрани да „влизат" в суитча директно с тагнат трафик. В конкретния пример обаче (в режим „Secure"), дори и клиентът да опита да влезе с някой от дефинираните VLAN-и, то това няма да му бъде разрешено, тъй-като за всички VID (освен неговия собствен) той е в режим „Drop".

При 'Secure' режим порт-базираната таблица с принадлежностите на портовете е без значение.

Също трябва да се отбележи, че в режим „Secure" и Default VID=1 за порт 6 – то през него не може да се „влезе" с нетагнат трафик, тъй-като на него ще се присвои VID=1, а той не е дефиниран и ще бъде филтриран.

7.4. Таг-базиран VLAN: Свързване на untag клиенти към 802.1q мрежа и прехвърляне на останалия трафик (тагнат/нетагнат) към друг порт

При горният пример видяхме, че освен описаните VLAN – останалите VID или нетагнат трафик се филтрират. Ако само се постави порт 6 в режим „Fallback": тогава, през порт 6 може да се влезе с нетагнат трафик и да се достъпят клиентските портове (също нетагнати). Тогава може чрез таблицата за порт-базираната принадлежност да се органични нетагнатия достъп до само определение портове.

Ако използваме тази функция можем да направим следната конфигурация: **входящият към суитча трафик на порт 6 го извеждаме през порт 5 към следващ магистрален суитч, а към ънтагнатите клиентските портове 1-4 извеждаме VID 100,200,300,400. Така обединяваме магистрална функция с функцията на краен суитч в мрежата.**

За тази цел двата „магистрални" порт 5 и 6 са в режим 'Fallback':

Per port settings for 802.1q and port-based VLAN

Port	802.1Q mode *	INGRESS pass mode **	EGRESS pass mode	EGRESS mode for port-based	Default VID for untagged	Force Default VID
Port 1	Secure	All	All	Untouch	100	☐
Port 2	Secure	All	All	Untouch	200	☐
Port 3	Secure	All	All	Untouch	300	☐
Port 4	Secure	All	All	Untouch	400	☐
Port 5	Fallback	All	All	Untouch	2	☐
Port 6	Fallback	All	All	Untouch	1	☐

* 'Port-base'=Disable 802.1q, use only port-based rules; 'Fallback'=Use port-based rules for undefined VIDs; 'Check'=Allow alien VIDs, drop undefined; 'Secure'=Drop alien and undefined VIDs
** INGRESS pass mode works in both 802.1Q and port-based modes!

802.1Q VIDs and egress port settings (applicable only when 802.1Q mode is 'Check' or 'Secure')

Enabled	VLAN's ID	Port Membership EGRESS rule					
		Port 1	Port 2	Port 3	Port 4	Port 5	Port 6
☑	100	Untag	Drop	Drop	Drop	Drop	Tag
☑	200	Drop	Untag	Drop	Drop	Drop	Tag
☑	300	Drop	Drop	Untag	Drop	Drop	Tag
☑	400	Drop	Drop	Drop	Untag	Drop	Tag
☐	0	Pass	Pass	Pass	Pass	Pass	Pass
☐	0	Pass	Pass	Pass	Pass	Pass	Pass
☐	0	Pass	Pass	Pass	Pass	Pass	Pass
☐	0	Pass	Pass	Pass	Pass	Pass	Pass

Port-based VLAN Members (applicable only when 802.1Q mode is 'Port-based' or 'Fallback')

	Port 1	Port 2	Port 3	Port 4	Port 5	Port 6
Port 1	☐	☐	☐	☐	☐	☐
Port 2	☐	☐	☐	☐	☐	☐
Port 3	☐	☐	☐	☐	☐	☐
Port 4	☐	☐	☐	☐	☐	☐
Port 5	☐	☐	☐	☐	☐	☑
Port 6	☐	☐	☐	☐	☑	☐

Постъпващ на порт 6 тагнат трафик с VID за клиентските портове се насочва към тях по вече описания в предния пример начин. Постъпващ на порт 5 такъв

трафик също ще се насочи към клиентските портове, но в обратна посока няма да се върне през порт 5, тъй-като той е в режим „Drop” за VLAN-ите. Ако и той се сложи в режим „Tag”, то тогава порт 5 и 6 стават взаимозаменяеми.

Постъпващ нетагнат (на него му се присвоява „Default VID” 1 или 2 в примера) или тагнат с други VID (извън описаните клиентски) трафик на порт 5 или 6, поради режимът им „Fallback”, се подлага на порт-базираните правила, които в случая дават право на двата порт да си го обменят неограничено.

Всичко това позволява реално през суитча да преминат неограничено количество VID-та въпреки, че имаме на разположение само 8бр. за детайлно дефиниране.