NEOMONTANA ELECTRONICS

www.neomontana-bg.com

P i c o I P

Интегриран IP модул

с контрол и управление

през SNMP и WEB

Ръководство на потребителя

Документът обхваща версии след 4.097 на системния софтуер на PicoIP.
При по-стари версии може да няма определени функции и параметри!

rev. 2.02

08.04.2013

СЪДЪРЖАНИЕ

©2008-2012, НЕОМОНТАНА ЕЛЕКТРОНИКС

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!

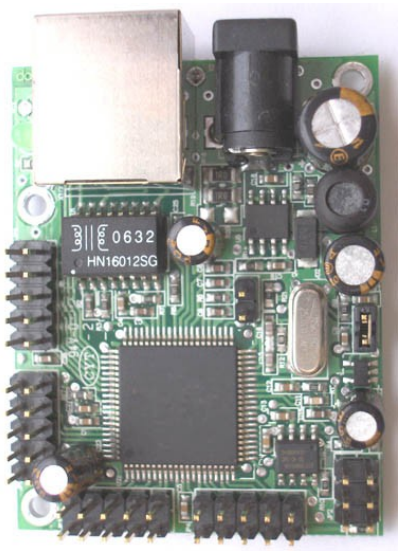
©2008-2012, НЕОМОНТАНА ЕЛЕКТРОНИКС

1. Версии на документа

Версия	Дата	Кратко описание на въведените промени
2.02	08.04.13	1. Добавени описания на функциите, достъпни от базова версия 4.100 (4.101,4.102) – изчитане на всички входно/изходни портове през един SNMP обект 2. Корекции в описанието на ping мониторинг режимите, свързано с отделянето на броенето на рестартите (PingCount) за всеки режим (входяю и изходящ) поотделно.
2.01	30.08.12	3. Добавени описания на функциите, достъпни от версия 4.097 – софтуерен ресет към фабрични настройки, Duplicate 'TargetRST' on P5 pins, зареждане през DHCP на TFTP IP и Remote IP to ping, инвертиране на действието при AnlogEvents. 4. Добавено Приложение 3 описващо използването на релейните комутатори с PicoIP 5. Добавено Приложение 4 даващо най-общи насоки при работа с SNMP
2.00	30.08.11	6. Цялостна промяна на документа, съобразно новите функции във версия 4.094 на PicoIP 7. Обобщаване на управлението на суитчове до всички предлагани модели суитчове 8. Разширен раздела за обновяване на системния софтуер през TFTP
1.09	01.04.11	9. Променени и добавени параметри във връзка с хардуерна версия v1.2 на PicoIP - защита от обратно захранващо напрежение - втори светодиод - конектор за извеждане на 12VDC към друга платка (при вграждане)
1.08	21.01.09	10. Добавена е втора бележка относно връщането на по-стари фърмуерни версии в раздела „Обновяване на системния софтуер през TFTP“
1.07	29.09.08	11. Добавени бележки относно възстановяване на фабричните настройки и промяната на мрежовите параметри през SNMP. 12. Добавено описание на „Analog Events“ 13. Добавено описание на „SNMP/Web Access Network“
1.06	14.08.08	1. Коригирана е неточност в описанието на портовете JP4 и JP3.
1.05	01.02.08	1. Премахнато е описанието на параметрите за настройка на суитч. Те са обособени в документацията на суитчовете.
1.04	25.09.07	1. Добавена е бележка относно дължината на рестартиращия импулс и времето на мониторинг режимите (5.9.3)
1.03	25.04.07	1. Добавено описание на функцията “Save I/O states” във версия 4.071 (7.3) 2. Променено е времето на автоматично обновяване на HTML страницата със статуса на портовете от 5 на 10s. Промяната е фактически приложена от версия 4.071
1.02	01.02.07	1. Добавена втора бележка относно последователното рестартиране (5.9.4)

©2008-2012, НЕОМОНТАНА ЕЛЕКТРОНИКС

2. Въведение



PicoIP компактно, автономно мрежово устройство, което има стандартен 10Mb/s Ethernet интерфейс. ***PicoIP*** е наследник на придобилият популярност ***TinyIP*** модул, като поддържа всички негови функции, но са добавени и множество нови.

Поддържаните от ***PicoIP*** протоколи са:

- Задължителните мрежови протоколи ARP, IP, ICMP (ping);
- DHCP - протокол за динамично конфигуриране на мрежовите настройки (IP, Network Mask, Gateway);
- 802.1q VLAN поддръжка с възможност за работа в пълния 12bit VLAN обхват;
- SNMPv1 (snmpget, snmpset) протокол за достъп до всички параметри и функции на модула;
- Генериране на SNMP-Trap съобщения при промяна на аналогови входове или промяна на състоянието на порт на суитч;
- Генериране на изходни сигнали при промяна на аналоговите входове;
- TCP/IP стек с Web Server за достъп до всички параметри и функции на модула;
- Режим на оторизация на Web достъпа и заключване по една Web сесия;
- Възможност за забрана на достъпа по SNMP за конфигуриране. Възстановяването е възможно само хардуерно;
- Възможност за забрана на достъпа по SNMP/Web по мрежа (IP/Mask);
- Възможност за спиране на Web достъпа;
- TFTP клиент за обновяване на системния софтуер на ***PicoIP*** (firmware update)

PicoIP разполага със следните хардуерни възможности:

- 8+8 цифрови входове/изходи, достъпни през SNMP и Web;
- 8 аналогови (цифрови) входа (10bit ADC, Vref=3.3V), достъпни през SNMP и Web;
- Допълнителен 8 канален I/O порт за управление на суитчове, рестартиране на външни устройства, функция „Ping Led” и др.;
- Хардуерен RS-232 порт (не е имплементиран в системния софтуер);

С помощта на ***PicoIP*** успешно се решават следните задачи:

- Активен мониторинг на мрежови сегменти и трасета;
- Рестартиране (ръчно или автоматично) на блокирало мрежово оборудване – модеми, безжични устройства, суитчове;
- Измерване на аналогови величини – напрежения, токове и др.;
- Управление/конфигуриране на суитчове;
- Изграждане на системи за автоматично следене и управление на различни технологични процеси и системи.

©2008-2012, НЕОМОНТАНА ЕЛЕКТРОНИКС

3. Сравнение между *PicoIP* и *TinyIP*

3.1 Технически и функционални възможности

В следващите две таблици са представени основните технически параметри и функционални възможности на двата модула, както сравнителен анализ. За подробно описание на конкретни функции на ***PicoIP*** трябва да се обърнете към следващите раздели.

Таблица 1. Сравнителна таблица за техническите характеристики на двата модула

Параметър	*PicoIP*	*TinyIP*	Забележка
Размери на модула	43x55mm	57x59mm	
Захранващо напрежение на модула	6 – 25VDC	7.5 – 12VDC	
Тип на захранващия преобразувател	Импулсен с високо КПД	Линеен	
Захранващо напрежение на CPU /ниво на лог. 1 на изхода/	3.3V	3.6V	
Брой цифрови изходи	16	8	
Аналогови входове	8/10bit ADC, Vref=3.3V/	3 /12bit ADC,Vref=1.5V/	
Цифрови входове	8 [1)]	8	
Хардуерен RS-232 порт[2)]	1	1	
Порт за управление на суитч	Да, отделен	Да, споделен с 4 от цифровите входове	
Джъмпер за възстановяване на фабричните настройки	Да	Да	При ***PicoIP*** джъмперът е единичен, в нормално състояние без поставен джъмпер
LED индикатор /Link, Activity, Power On/	Да	Да	
Допълнителен LED индикатор	Да[3)]	Не	
Вграден датчик за температура	Не	Да	

1) Цифровите входове са реално аналоговите входове, като изкуствено се конвертира входното напрежение в логически нули и единици;
2) Не е имплементиран в системния софтуер;
3) Поставен във хардуерна версия 1.2

©2008-2012, НЕОМОНТАНА ЕЛЕКТРОНИКС

Таблица 2 Сравнителна таблица за функционалните възможности на двата модула

Параметър / Протокол	*PicoIP*	*TinyIP*	Забележка
ICMP Echo Reply /отговор на ping/	Да /до 1460 байта/	Да /винаги с 22 байта/	Не се поддържат фрагментирани IP пакети
ICMP Echo Request /Ping към даден адрес/	Да	Не	
Функция „Ping Timeout Restart" при липса на входящ ping /Echo Request/	Да	Да	
Функция „Ping Timeout Restart" при липса на отговор на ping към произволен IP адрес /Echo Reply/	Да	Не	
Задаване дължината на рестартиращи импулс	Да /х 250мс/	Да /х 42мс/	
Задаване лимит на последователните рестартирания	Да	Да	
Режим нулиране на изходните I/O пинове при ping timeout /Reset I/O ports on ping restart/	да	да	
LED индикатор за входящ пинг /ICMP Echo request LED/	Да	Да	
Запазване на състоянието на I/O портовете /Save I/O states/	Да /от версия 4.071/	Да	
Динамично конфигуриране на мрежовите параметри DHCP	Да	Не	
Статично конфигуриране на мрежовите параметри	Да	Да	
Мрежови параметри	IP, Network Mask, Default Gateway	IP address	
802.1q VLAN	Да	Да	
MAC Lock	Да, 2 MAC адреса	Да, 2 MAC адреса	
SNMPv1	Да /snmpget, snmpset/	Да /snmpget, snmpset/	
Блокиране на достъпа през SNMP до конфигурационните параметри	Да	Да	

©2008-2012, НЕОМОНТАНА ЕЛЕКТРОНИКС

Параметър / Протокол	*PicoIP*	*TinyIP*	Забележка
Read-Write Community String	Да	Да	
Read-Only Community String	Да	Не	
Генериране на SNMP traps към отдалечен адрес	Да	Не	Генерират се при промяна на аналогов вход извън определен интервал или при промяна на статуса на порт (Up/Down) на суитч
Разширен набор от SNMP команди за достъп до I/O портовете	Да	Не	Възможност за побитов достъп до всеки порт
Разширен набор SNMP команди за конфигуриране/статус на ***SmartSwitch***	Да	Не	Достъп до всички параметри на ***SmartSwitch*** с команди от високо ниво, а не само чрез бинарен достъп
Стандартен /бинарен/ достъп до конфигурацията на ***SmartSwitch***	Да	Да	Съвместима с WinTic
Вграден Web сървър за конфигурация/достъп	Да	Не	Поддържа един потребител/сесия. Достъп само с име/парола (basic authentication). Заключване към текущата сесия.
TFTP клиент за обновяване на системния софтуер	Да	Не	
Команда за стартиране на TFTP обновяването (SNMP, Web)	Да	Не	
Възможност за забрана на командата за TFTP обновяване	Да	Не	
Управление на суитчове	Да	Да	TinyIP може да управлява САМО ***SmartSwitch***
Функция “SmartApply” – потвърждаване на всяка конфигурация	Да /чрез Web или SNMP/	Да /чрез SNMP/	

3.2 Замяна на *TinyIP* с *PicoIP* при конкретни приложения

Основен принцип при проектирането на ***PicoIP*** е запазването на неговата съвместимост с ***TinyIP***. Съвместимостта е наложителна, особено на ниво достъп до модула, за да не се налага промяна във вече разработени приложения за достъп до ***TinyIP***. За това всички досегашни SNMP команди са запазени, като единствено е необходимо пресвързване на съответните входно/изходни сигнали към новите портове на ***PicoIP***. Тези особености при свързването са предмет на този раздел.

3.2.1 Управление на *SmartSwitch*

Единствената разлика между двата модула е в кабела за връзка към ***SmartSwitch*** и естествено мястото на неговото поставяне на ***PicoIP***. За повече

©2008-2012, НЕОМОНТАНА ЕЛЕКТРОНИКС

информация можете да се обърнете към документа „Интегриране на ***PicoIP*** към ***SmartSwitch***”.

3.2.2 Рестартиране на външно устройство (Target Restart)

За рестартирането на външно устройство, независимо дали ръчно или автоматично (при липса на ping), се използва специален изход на ***PicoIP*** – “TargetRST”, който се намира на системния порт JP6 (виж. Приложение 1). Не е необходимо никакво допълнително конфигуриране на ***PicoIP*** за работата на този пин, тъй-като той е изцяло заделен само за тази функция. (т.е. наличните при ***TinyIP*** различни варианти на конфигурация на рестартиращите пинове между външното устройство и ***SmartSwitch*** вече не са необходими).

От версия 4.097 е въведена възможност сигналът “TargetRST” да се мултиплицира на P5 (JP4). Това позволява гъвкавото му разпределяне на няколко изхода, което улеснява използването на функцията при интегриране с външни релета. Също така, при повреда на пина на JP6 за тази функция – лесно може да се използва друг свободен изход на P5. При използване на функацията за мултиплициране на “TargetRST” единствено трябва да се уверите, че съответните пинове на P5 са конфигурирани в режим „Output”.

3.2.3 Използване на цифровите изходи (за управление на външни устройства)

По отношение на цифровите изходи е налице съвместимост между ***TinyIP*** и ***PicoIP***: портовете на ***PicoIP*** обозначени като P3 и P5 (Приложение 1) съответстват на същите логически портове на ***TinyIP***. С други думи всеки до сега използван изходен пин на ***TinyIP*** може директно да се свърже на същия порт и място на ***PicoIP***. Командите по SNMP за достъп до пина трябва да останат в досегашния си вариант.

3.2.4 Използване на аналоговите входове за цифрови сигнали

При входовете ситуацията е малко по-усложнена. Това се налага поради факта, че при ***PicoIP*** е налице един общ входен порт – P6, на който всички пинове са входни. На практика този порт е изцяло аналогов с 10bit АЦП. Той може да се използва както за измерване на аналогови напрежение в обхвата 0 до 3.3V и да се получават директно данни за измереното напрежение в цифров вид, така и да се използва като цифров входен порт, като цифровите състояния се измерват по аналогов път и се конвертират в лог. 0 или 1 в зависимост от обхвата на напрежението.

На следващата таблица е показана връзката между входен пин на ***TinyIP*** и неговият съответен при ***PicoIP***. При тази на пръв поглед сложна схема на замяна на пиновете е съхранен формата на данните за състоянието на входните пинове, получавани през SNMP.

Таблица 3 Връзка между входните пинове на двата модула

TinyIP		***PicoIP***	
Порт	**Входен пин**	**Порт**	**Входен пин**
P3	5	P6	2
	6		4
	7		6
	8		8
P5	1		1
	3		3
	5		5
	7		7
P6	4 (P6.3)		4
	6 (P6.5)		6
	8 (P6.7)		8

©2008-2012, НЕОМОНТАНА ЕЛЕКТРОНИКС

3.2.5 Използване на аналоговите входове за измерване на аналогови сигнали

Осемте входа на P6 могат да се използват за директно измерване на аналогови величини. За да се запази съвместимостта с ***TinyIP*** командите по SNMP за изчитане на аналоговите входове (P6.3, P6.5, P6.7) са запазени във същия формат и при ***PicoIP***, като резултатът е конвертиран от 10 на 12bit и е преизчислен за опорно напрежение 1.5V.

По този начин към съответните входове на ***PicoIP*** могат директно да се свържат същите източници на аналогово напрежение, използвани с ***TinyIP*** и измерването да бъде със същият обхват, без да се налага допълнително преизчисляване.

Използването на софтуерно конвертиране от 10 на 12bit, както и приравняването на резултата към друго опорно напрежение води до поява на грешка в измерването – младшите два бита реално не отразяват стойността на измерваната величина.

За използване на пълните възможности на аналоговите входове трябва да се използват специално заделените нови SNMP команди за достъп до всеки отделен пин на входния порт P6.

©2008-2012, НЕОМОНТАНА ЕЛЕКТРОНИКС

4. Достъп до параметрите и функциите на *PicoIP*

Настройката на всеки един параметър на ***PicoIP*** е възможна през SNMP и през Web. Има и параметри, които са достъпни само през WEB (например „Port Labels").

4.1 Достъп през SNMP

В ***PicoIP*** е заложена поддръжка на основните за SNMPv1 команди: snmpget и snmpset. С тяхна помощ могат да бъдат прочетени или променени стойностите на конфигурационните параметри. Те са описани детайлно в специален MIB файл: „***PicoIP***-MIB.txt".

За достъп през SNMP се използват две пароли (community string): Read-Only Community String и Read-Write Community String. С първата е възможно само четене на параметрите, а с втората и тяхната промяна.

Примерна SNMP заявка за получаване на IP адреса на ***PicoIP***:

- snmpget -v1 -c 000000000000 172.16.100.2 1.3.6.1.4.1.19865.1.1.1.0
  SNMPv2-SMI::enterprises.19865.1.1.1.0 = IpAddress: 172.16.100.2

или (в случай, че е инсталиран .mib файла към библиотеката net-snmp)

- snmpget -v1 -c 000000000000 172.16.100.2 cfgIP.0

Фабричните стойности на паролите са посочени в параграф 10.

При използване на SNMP за достъп, да се използват snmpget и snmpset само към един OID, а не към група от OIDве. Други команди (snmpwalk например) не се поддържат!

*ВАЖНО!!! Поради спецификата на SNMP протокола, който се поддържа от **PicoIP** (невъзможност за едновременен достъп до няколко OID), първоначалната настройка на IP/Mask/Gateway е желателно да се направи през Web страницата на **PicoIP**. В противен случай може да се окаже невъзможно задаването на желаните настройки, поради ограничението за промяната им поединично.*

4.1.1 Промяна на UDP порта на SNMP сървъра в *PicoIP*

От версия 4.094 е възможно потребителят да промени входящият порт на SNMP сървъра в ***PicoIP*** от 161 (UDP) на произволен порт от 1025 до 65535. Опитът за задаване на порт в обхвата 1-1024 ще бъде възприето като порт 161. Промяната на този параметър води до рестартиране на ***PicoIP***.

SNMP: Промяна на cfgSNMPport.0
Web: Меню „Setup->SNMP settings/Listen on UDP port "

4.2 Достъп чрез Web браузер

Освен през сравнително сложния SNMP метод за достъп, системните параметри на ***PicoIP*** могат да бъдат настроени и със стандартен браузер (IE, Mozilla, NetscapeNavigator и др.). За предпочитане е да се използва Mozilla Firefox.

За ограничаване на достъпа до вграденият в ***PicoIP*** Web Server е заложен стандартен механизъм на оторизация с потребител/парола (Basic Authentication). Фабричните стойности на потребителя/паролата (параграф 10) е желателно в последствие да бъдат променени.

Web сървърът разполага с една единствена сесия – т.е. в даден момент от времето е възможен достъп до него само от един IP адрес. Сесията има таймаут около 60s, през който ако няма активен достъп от адреса, тя се приключва и се дава възможност за достъп от нов (или от последния) IP адрес. Всичко това е направено с цел сигурност и надеждност на работа. Освен това едновременният достъп от няколко потребителя, които променят системни настройки би довел до получаване на непредвидена системна (или на суитча) конфигурация.

©2008-2012, НЕОМОНТАНА ЕЛЕКТРОНИКС

4.2.1 Промяна на HTTP порта на *PicoIP*

От версия 4.094 е възможно потребителят да промени порт 80 за HTTP достъпа на произволен порт от 1025 до 65535. Опитът за задаване на порт в обхвата 1-1024 ще бъде възприето като порт 80. Промяната на този параметър води до рестартиране на ***PicoIP***.

Достъпът до ***PicoIP*** след смяна на прорта трябва да бъде от вида http://172.16.100.2:port

SNMP: Промяна на cfgHTTPport.0
Web: Меню „Setup->Miscellaneous/ Web server ...on port ”

5. Конфигурационни параметри и основни системни функции

В този раздел са описани различните системни функции и протоколи, които поддържа ***PicoIP***. Към всяка функция са поместени и съответните имена на OID-овете, чрез които те са достъпни за SNMP достъп, както и съответното меню->поле на Web страницата при достъп през браузер.

5.1 Стандартни протоколи

PicoIP поддържа стандартните протоколи ARP и ICMP (echo request/reply). Те не разполагат с конкретни параметри за настройка/конфигуриране.

5.2 802.1q VLAN

PicoIP може да работи с нормални или с тагнати пакети (IEEE 802.11q). Поддържа се пълният набор от 12bit VLAN тагове.

SNMP: Промяна на съответния бит в cfgMode.0 и задаване на съответния VLAN таг в cfgVLANTag.0
Web: Меню „Setup->Tagged VLAN mode" и „Setup->VLAN ID"

*Работата на **PicoIP** във режим с тагнати пакети е **силно препоръчителна**, тъй-като **PicoIP** филтрира хардуерно тагнатия от нетагнат трафик. По този начин той се разтоварва от обработката на огромно количество ненужен мрежов трафик. Освен това, работата във VLAN позволява и повишаване на сигурността при достъпа до модула.*

5.3 DHCP или статично конфигуриране

Мрежовите параметри (IP, Mask, Default Gateway) могат да бъдат получени от ***PicoIP*** динамично, ако има конфигуриран DHCP сървър. При липсата на такъв те могат да бъдат зададени статично от потребителя.

Разрешаването/спирането на DHCP клиента става от:
SNMP: Промяна на съответния бит в cfgNewMode.0
Web: Меню „Setup-> DHCP client"

*Разрешаването на DHCP клиента при липса на работещ сървър (или наличие на мрежов проблем) може да доведе до невъзможност на **PicoIP** да зареди мрежовите си параметри и по този начин достъпът до него да се загуби. За да се предотврати това **PicoIP** изчаква определен период от време (около 40s след рестартирането си) за да получи мрежовите си настройки. В случай, че не успее, **PicoIP** зарежда последно настройваните си статични параметри и започва да работи с тях, като същевременно продължава да търси DHCP сървър. Ако се получи отговор от сървър **PicoIP** мигновено възприема новите си динамични параметри.*

От версия 4.097 е предвидена възможност през DHCP да могат да се провизират допълнително IP адресът на TFTP сървъра и на устройството, което се следи чрез изходящ Ping. За тази цел се използват две от стандартно и рядко използвани опции в DHCP:

option www-server – за IP адреса на отдалеченото устройство;

option swap-server – за IP адреса на TFTP сървъра, който съдържа имиджа за софтуерно обновяване.

Следния пример накратко илюстрира настройките в dhcpd.conf (Linux/Debian) за динамично конфигуриране в мрежа 192.168.1.0, като на определен PicoIP (pico_test, разграничава се по MAC адреса) са индивидуално фиксирани IP, RemoteIP, TFTP server.

©2008-2012, НЕОМОНТАНА ЕЛЕКТРОНИКС

File: dhcpd.conf (partitial content)

```
#
# Sample configuration file for ISC dhcpd for Debian
#
# $Id: dhcpd.conf,v 1.4.2.2 2002/07/10 03:50:33 peloy Exp $
#
# option definitions common to all supported networks...

option subnet-mask 255.255.255.0;
default-lease-time 600;
max-lease-time 7200;

subnet 192.168.1.0 netmask 255.255.255.0 {
        range 192.168.1.160 192.168.1.175;
        option domain-name-servers 192.168.1.1;
        option routers 192.168.1.1;
        option subnet-mask 255.255.255.0;
        default-lease-time 3600;
        max-lease-time 7200;
}

host pico_test {
  hardware ethernet ec:f2:36:00:0b:db;
  fixed-address 192.168.1.158;
  option www-server 192.168.1.156;
  option swap-server 192.168.1.104;
}
```

5.4 Мрежови параметри

Това са основните параметри на ***PicoIP***, от които зависи достъпът до него. Тези параметри включват IP адрес, Мрежова маска (Network Mask) и шлюз за достъп до външни мрежи (Default Gateway).

SNMP: cfgIP.0, cfgNetMask.0, cfgDefGW.0
Web: Меню „Setup->IP address”, „Setup->Subnet Mask”, „Setup->Default Gateway”

*Статичните параметри се съхраняват в енергонезависима памет в **PicoIP**. Те не се променят от DHCP параметрите. При достъп през Web и разрешен DHCP режим в полетата на съответните параметри се изписват данните, получени от DHCP сървъра, а не статично зададените такива!*

5.5 Защита на достъпа по MAC адрес

PicoIP дава възможност за глобално (всички протоколи) ограничаване на достъпа до него от други устройства, чрез задаване на техния MAC адрес. Защитата може да бъде към до два MAC адреса. Нейното деактивиране става, чрез задаване и на двата MAC адреса като нулеви (000000000000).

SNMP: cfgMACLock1.0, cfgMACLock2.0
Web: Меню „Setup-> Access MAC address 1” и „Setup-> Access MAC address 2”

При използване на защита по MAC адрес, да се има предвид, че при достъп от външни мрежи, към модула пристигат пакети с MAC адреса на Default Gateway. В такъв случай той трябва да бъде винаги зададен като един от двата защитни адреса.

5.6 Защита на достъпа през SNMP/Web по IP

Тази функция дава възможност за дефиниране на една мрежа (IP/MASK), която единствено има достъп до PicoIP през SNMP и Web. Функцията е предназначена за филтриране и защита на достъпа до модула не само на ниво MAC адреси, но и на ниво IP адреси.

©2008-2012, НЕОМОНТАНА ЕЛЕКТРОНИКС

Филтрирането засяга единствено SNMP и Web достъпа, всички останали протоколи ARP, ICMP, DHCP не се филтрират.

SNMP: cfgAccessIP.0, cfgAccessMask.0
Web: Меню „Setup-> Network IP ” и „Setup-> Network Mask ”

*Функцията е въведена от версия 4.078 на системния софтуер на **PicoIP**.*
Защитата по MAC адрес е с ПО-ВИСОК приоритет от тази по IP/MASK!
При промяна през SNMP на параметрите на мрежата първо настройвайте IP адреса при отворена маска (0.0.0.0), а след това маската. В противен случай (при смяна първо на IP адреса, при някаква зададена маска) е възможно да се получи нежелана конфигурация от IP/MASK, която да спре достъпа до модула и да направи невъзможно задаването на правилната маска.

5.7 Забрана за достъп до системните настройки на *PicoIP* през SNMP

Тази опция дава възможност да се преустанови достъпът до настройките от групата „Configuration.xxxx.0” – т.е. това са основните системни настройки на модула. Достъпът до портовете на модула, неговото рестартиране и управление на ***SmartSwitch*** се запазват.

Тази забрана не може да бъде снета чрез SNMP команда, а единствено през Web (ако е разрешен Web достъпът) или чрез хардуерна инициализация на модула към фабрични настройки.

Основната идея на този режим е предотвратяване на злонамерена промяна на настройките на модул, който е поставен в реални условия и на практика няма нужда от повече промени в настройките.

SNMP: Промяна на съответния бит в cfgMode.0
Web: Меню „Setup-> SNMP access to IP configuration”

5.8 Пароли за достъп през SNMP (Community strings)

Двете пароли са необходими при изпълняване на SNMP команди и определят права на достъп само за четене или за четене и запис. Могат да съдържат от 4 до 12 произволни символи.

SNMP: cfgPassword.0 и cfgReadOnlyPassword.0
Web: Меню „Setup-> SNMP read-write community string” и „Setup-> SNMP read-only community string”

Паролата за запис/четене не е достъпна за четене през SNMP.

5.9 Мониторинг режими, базирани на ICMP ping

PicoIP разполага с двупосочен (входящ/изходящ) режим за мониторинг чрез получаване/изпращане на ICMP Echo Request и ICMP Echo Reply пакети. С тази функция ***PicoIP*** лесно се превръща в средство за активен мониторинг на мрежови трасета и устройства. Освен мониторинга ***PicoIP*** изработва рестартиращ импулс при липса на отговор.

С общ параметър се задава времето (в минути) през което трябва да се получи заявка/отговор. Изтичането на времевия период за мониторинг режим без получаване на съответната заявка/отговор води до рестартиране на суитча (ако е зададено) и на външно устройство (ако е зададено).

SNMP: cfgPingTime.0 (в минути)
Web: Меню „Setup-> Timeout”

©2008-2012, НЕОМОНТАНА ЕЛЕКТРОНИКС

5.9.1 Входящ ICMP мониторинг

При разрешен входящ мониторинг ***PicoIP*** очаква получаването на ping от произволен IP адрес в рамките на зададения времеви интервал.

SNMP: Промяна на съответния бит в cfgMode.0
Web: Меню „Setup-> Restart on incoming ping timeout”

*При тежък мрежов трафик е напълно нормално **PicoIP** да не получи пакети, изпратени към него. Поради това, за да може този мониторинг режим да работи надеждно, е необходимо в зададения времеви интервал да се изпращат поне 5-10 ping заявки към **PicoIP**.*

5.9.2 Изходящ ICMP мониторинг

При изходящ мониторинг ***PicoIP*** генерира ping към зададения произволен IP адрес и очаква отговор от него в рамките на зададения времеви интервал. Генерирането на заявки става няколко пъти в минута.

Независимо, че използват общ параметър за настройка на времевия интервал, двата режима имат отделни таймери.

SNMP: Разрешаване чрез съответния бит в cfgNewMode.0, cfgMonitorIP.0
Web: Меню „Setup->Restart on remote IP timeout”, „Setup->Remote IP to ping”

Web интерфейса и SNMP показват реалната стойност на „MonitorIP” - т.е. при подадени опции през DHCP се показват динамичните стойности; при липса на DHCP или не зададени в DHCP опции се показват стойностите, които са в конфигурационната паметна на PicoIP (това са последно използваните статични стойности). Няма предвиден механизъм за определяне дали конкретната стойност е заредена от DHCP или от статичните настройките на PicoIP!

5.9.3 Рестартиране на външни устройства (Restart Target Device)

За рестартиране на външно устройство (през съответен драйвер, напр. Relay Board или RelayBox2x) при мониторинг режим се използва заделен специално за целта пин „Target RST” (виж Таблица 5). Така става възможно рестартирането и на произволни консуматори (включително на 220V), освен на суитч. От версия 4.097 е налична и възможнос за „размножаване“ на този сигнал и на изводите на P5 (JP4).

Рестартирането на външно устройство при мониторинг събитие може да бъде спряно/активирано от потребителя. Освен това е достъпно за задаване времето на рестартиращия импулс (лог. „1”) : (от 0 до 32767)x250ms.

Рестартирането на външното устройство може да се извърши и ръчно, чрез съответната команда.

SNMP: Промяна на съответния бит в cfgMode.0; cfgResetPulse.0, pctrlRestart.0 (read-only), cfgP5DupRST.0
Web: Меню „Setup->Restart external device”, „Setup->External device restart pulse width”, „I/O ports -> Force TargetRST”, „Setup->Duplicate 'TargetRST' on P5 pins”

Задаването на дължина на рестартиращия импулс по-голяма от времето “Ping Timeout” ще доведе до недефинирано (възможно е и безкрайно) удължаване на рестартиращия импулс, когато е налице липсата на съответния „ping” заявка или отговор за определения период от време. Причината за това е в цикличното запускане на рестартиращия импулс, по-често от колкото е неговата дължина!

5.9.4 Определяне на броя на последователните рестарти при мониторинг режимите

При трайна загуба на връзка или мрежов проблем мониторинг режимите ще започнат циклично рестартиране на разрешените устройства през зададения интервал от време. В случай, че не е необходимо безкрайното рестартиране, броят на последователните рестарти може да бъде ограничен в интервала 1 .. 255.

©2008-2012, НЕОМОНТАНА ЕЛЕКТРОНИКС

SNMP: Промяна на съответния бит в cfgResetCount.0
Web: Меню „Setup-> Number of consecutive restarts”

Стойността, който се задава на този параметър през SNMP е реално с единица по-малка от броя на рестартите (т.е. стойност 0 означава 1 рестарт).Задаването на стойност 255 означава неограничен брой рестартирания.

За версии преди 4.099: *При едновременна работа на входящ и изходящ ICMP мониторинг трябва да отпаднат и двете процеса за да работи коректно зададения брой на рестартите. Ако отпадне само единия режим, наличието на другия няма да позволява коректното отброяване на рестартите и те ще продължават неограничено, независимо от зададената стойност.*
За версии от 4.099 и по-нови: *отброяването на последователните растарти е независимо за входящ и изходящ ping и двата процеса не си вилят.*

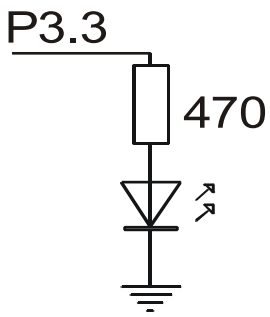
5.9.5 Нулиране на I/O портовете при мониторинг рестарт

С разрешаването на тази опция, ***PicoIP*** установява в лог. „0” всички изходи на P3 и P5 (виж Таблица 5), когато възникне рестартиране от мониторинг режим.

SNMP: Промяна на съответния бит в cfgNewMode.0
Web: Меню „Setup-> Reset I/O ports on ping restart”

5.10 Индикатор на входящи „ping” заявки „Ping LED”

Разрешаването на този режим, дава възможност ***PicoIP*** да се превърне в прост мрежов анализатор (при конкретни настройки на мрежата), който да индицира наличието на “ping” заявки към неговия IP адрес. Всяка получена заявка води до промяна на текущото състояние на изход “Ping LED” (виж Таблица 5). На схемата е показано примерно свързване на светодиод, директно към този пин.



SNMP: Промяна на съответния бит в cfgNewMode.0
Web: Меню „Setup-> Toggle JP6.4 on outgoing ping request”

5.11 Втори LED индикатор (за хардуерна версия 1.2)

Във хардуерна версия 1.2 на ***PicoIP*** е вграден втори светодиод за индикация на различни режими (достъпни от софтуерна версия 4.094+): „Power ON”, “Ping IN”, “Ping OUT”, “Ping BOTH”, “DHCP valid IP”.

SNMP: Промяна на съответния бит в cfgLED2mode.0
Web: Меню „Setup-> Second LED mode ”

5.12 Обновяване на системния софтуер през TFTP

PicoIP е снабден с TFTP клиент, който при подаване на команда се свързва към IP адреса на TFTP сървъра и изтегля (ако е наличен) необходимия му файл със обновление. След приключване на обновяването той се саморестартира.

След смяна на версията на фърмуера ЗАДЪЛЖИТЕЛНО ИЗЧИСТЕТЕ КЕША НА БРАУЗЕРА!!! В противен случай ще се получи смесване на нови със кеширани версии на WEB съдържанието, което ще доведе до грешки в управлението /конфигурирането на устройството!

©2008-2012, НЕОМОНТАНА ЕЛЕКТРОНИКС

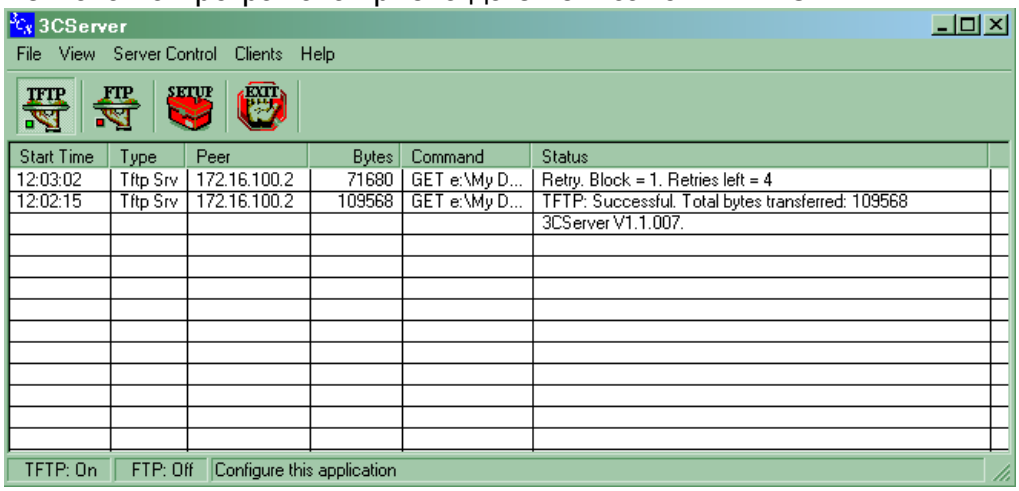
*Силно препоръчително е обновяването на ситемния софтуер да не се прави в реални условия (големи мрежи, дистанционно захранване и т.н.). Пропадането на захранването в момента на обновление на системния софтуер ще доведе до повреда в **PicoIP**.*

*Връщането на **по-стара версия** (т.нар. downgrade) в повечето случаи ще изисква еднократно последващо **зареждане на фабричните настройки**. Това също означава, че процесът не трябва да се прави в реални условия (отдалечено).*

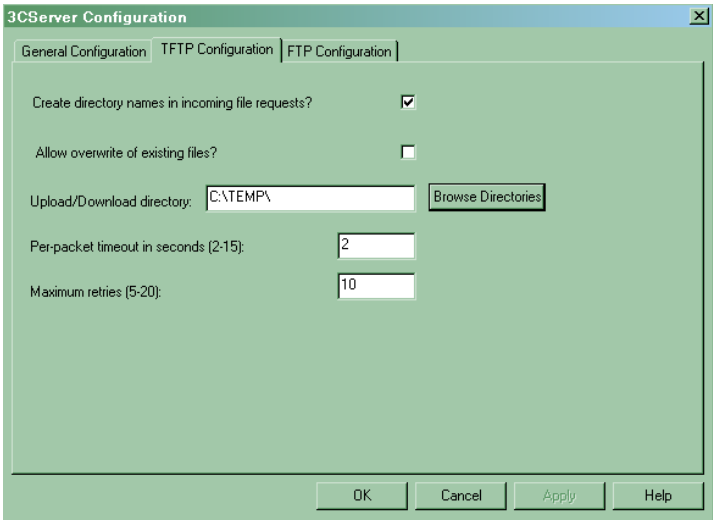
*Най-подходящо е ъпдейт на софтуера да се прави на **PicoIP**, на който са заредени фабричните настройки.*

За коректно протичане на процеса на обновяване трябва да се премине през следните стъпки:

1. Инсталирайте програмата '3CServer' (http://lan.neomontana-bg.com/download/3cs117.zip) за Windows. Може да се използват и други програми, включително и вградените в Linux TFTP демони.
2. Стартирайте програмата, пуснете с бутона „TFTP" сървъра. На статус лентата на програмата трябва да е изписано TFTP: On



3. Влезте в SETUP на програмата в частта TFTP Configuration:



Важно е да видите/зададете „Upload/Download directory" и там да поставите файла за ъпдейт „pipfw.bin". **Файлът трябва да е в самата директория, а не в поддиректории; името и разширението му НЕ трябва да се променят**. Настройте параметрите за таймаут и повторни опити, както е показано.

4. Уверете се, че инсталирани Firewall програми не блокират приложението.
5. ***PicoIP*** да бъде с разрешено обновяване през TFTP, правилно зададен съответния IP адрес на TFTP сървъра и коректни мрежови настройки.
6. Стартирайте обновяването – през WEB или SNMP.

©2008-2012, НЕОМОНТАНА ЕЛЕКТРОНИКС

НЕ ИЗКЛЮЧВАЙТЕ *PicoIP* ПО ВРЕМЕ НА ТОЗИ ПРОЦЕС!!!

7. В статус прозореца трябва да видите информация за започналия обмен на файла със съответното количество прехвърлена информация. Нормално е при някои порции данни да получите съобщения за „Timeout" и „Retry" - това не трябва да Ви притеснява, ако след това прехвърлянето на данните си продължи само.
8. След като приключи прехвърлянето („TFTP successfull ...") ***PicoIP*** ще се саморестартира.
9. Влезте в Web или WinTIC – вече трябва да се изписва новата фърмуерна версия, който сте заредели. При достъп през WEB се уверете, че зареждате „пресни" версии на WEB съдържаниет – най-добре изчистете кеша на браузера.

При липса на връзка към сървъра ***PicoIP*** прави няколко опита за установяването преди окончателно да приключи изпълнението на командата без обновяване.

SNMP: Промяна на съответния бит в cfgNewMode.0 за разрешаване на обновяването през TFTP; cfgTFTPServerIP.0 и cfgUpdateFirmware.0 (read-only)

Web: Меню „Setup-> TFTP firmware update", „Setup->TFTP server IP address", „Firmware Update"

5.13 Управление на предлаганите от НЕОМОНТАНА ЕЛЕКТРОНИКС суитчове

По подразбиране управлението на суитч през PicoIP е спряно. То трябва да бъде разрешено (Switch Control = Enable) от Web или SNMP на всяко новозакупено или с фабрични настройки устройство!

PicoIP се продава с фабрично заложен софтуер за управление на SmartSwitch (SS208-POE). Ако е необходимо да се управлява/програмира друг модел суитч е необходимо да се смени през TFTP системния фърмуер на PicoIP със съответния за модела суитч. Всички фърмуери са достъпни за свободен download и могат да се сменят неограничено.

В този режим на работа ***PicoIP*** се превръща и в „management" ядро за достъп до многобройните функции управляемите суитчове (***SmartSwitch, CleverSwitch, NMGS4P1F, NMGS5Pv2 ...)*** - контрол на портове, VLAN групиране, статус, тагване и разтагване и т.н. При постоянно свързани ***PicoIP*** и суитч те се превръщат в „managed switch" със собствен IP адрес и on-line достъп (Web и SNMP). Възможно е и използването на ***PicoIP*** само като „програматор" за зареждане на определена статична конфигурация в суитча без да е необходимо след това двете устройства да работят съвместно. Разбира се, по този начин престава да съществува on-line достъпа до суитча през мрежата.

Съвместната работа на двете устройства има и същественото предимство, че ***PicoIP*** може да извършва мониторинг и да рестартира и самия суитч при наличие на мрежов проблем (виж 5.9). В допълнение ***PicoIP*** може да генерира и SNMPtraps при промяна на статуса на портове на суитча.

За подробности по съвместната работа на двете устройства вижте раздел 6. Пълно описание на възможностите на суитчовете можете да намерите в техните описания.

SNMP: Промяна на съответния бит в cfgMode.0

Web: Меню „Setup-> Switch control"

©2008-2012, НЕОМОНТАНА ЕЛЕКТРОНИКС

5.14 Забрана на достъпа през Web

Вграденият в ***PicoIP*** Web сървър може да бъде забранен с тази опция. Препоръчително при поставянето на ***PicoIP*** в реални условия да не се ползва Web достъпа, тъй-като натоварва значително ***PicoIP*** по обработката на Web съдържанието и на TCP/IP стека.

SNMP: Промяна на съответния бит в cfgNewMode.0
Web: Меню „Setup-> Web server”

*Web достъпът може да бъде пуснат повторно само чрез SNMP команда (и разбира се след зареждане на фабрични настройки – раздел 10).Ако обаче е забранен достъпът през SNMP до системните параметри на **PicoIP** (раздел 5.6) то повторното разрешаване на Web сървъра остава възможно единствено чрез хардуерно зареждане на фабричните настройки.*

5.15 Забрана на обработка на Broadcast фреймове

В този режим ***PicoIP*** не обработва и не отговаря на фреймове с MAC адрес на получателя FF-FF-FF-FF-FF-FF. Използването на този режим позволява ***PicoIP*** да се „скрие” от околния свят (тъй-като няма да отговаря на ARP заявки) и същевременно да се разтовари от обработката на Broadcast трафик, който по начало е трудно контролируем в големи мрежи.

SNMP: Промяна на съответния бит в cfgMode.0
Web: Меню „Setup-> Broadcast frames”

Използването на този режим да става само от потребители, които имат задълбочени познания по функционирането на мрежите и съответните протоколи (ARP, DHCP) на ниско ниво!

©2008-2012, НЕОМОНТАНА ЕЛЕКТРОНИКС

6. Управление на суитчове

За подробна информация за достъпните параметри за конфигуриране на различните модели суитчове се обърнете към техните описания на http://lan.neomontana-bg.com. Тук само на кратко са описани възможните методи на достъп

6.1 Достъп през Web

За достъп до различните параметри на суитчовете, предлагани от НЕОМОНТАНА ЕЛЕКТРОНИКС, през Web е обособена отделна категория от Web страницата – „Switch Control”.

6.2 Достъп през SNMP

*PicoIP поддържа SNMP достъп единствено за **SmartSwitch (SS208-POE)**. За всички останали модели суитчове може да се използва само WEB за управлението и конфигурирането им.*

Всички описани опции за конфигуриране на ***SmartSwitch*** 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 използване.

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)

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 суитч, когато към него е свързан и Ethernet линка на ***PicoIP***. Такова конфигуриране би могло да прекрати достъпа до модула през мрежата и да го направи изцяло недостъпно on-line за администратора.

“Smart Configuration Apply” се грижи за това да провери дали след реконфигурирането на суитча 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 суитча, 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 суитча на фабричните настройки и неговото рестартиране.

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 сервъра (например страницата за статус на портовете).

Задействането на този механизъм временно (до изтичане на 2min или до потвърждаване на настройките по един от описаните начини) преустановява рестартирането на суитча в следствие на ICMP мониторинг събития.

©2008-2012, НЕОМОНТАНА ЕЛЕКТРОНИКС

7. I/O портове (аналогови/цифрови)

PicoIP разполага с 8+8 цифрови вход/изхода и 8 аналогови входа (виж 11). Аналоговите входове могат да се използват и като цифрови. Достъпът е възможен през SNMP и през Web. Портовете са условно означени като P3, P5 и P6.

7.1 Определяне на портовете като вход или изход

От версия 4.094 ***PicoIP*** дава възможност всеки от 16-те цифрови изходи на P3 и P5 да бъдат конфигурирани като цифрови входове. Цифровите входове автоматично става достъпни при четене на досегашните OID за изчитане на изходите – не е необходима друга допълнителна настройка.

SNMP: Промяна на съответния бит в cfgP3Dir.0, cfgP5Dir.0 (1=Out,2=In)
Web: Меню „Setup-> I/O ports settings”

7.2 Конфигуриране на Pull-Up/Pull-Down за цифровите входове

Тъй-като цифровите входове са „висящи“ и нямат установено ниво, когато не са свързани е предвидена възможност да се активират вътрешни „pull-up” или „pull-down” на всеки един вход. Активирането им е приблизително еквивалентно на свързване на резистор към +3.3V или 0V съответно със стойност около 50kOm.

На потребителя се предоставя възможността глобално да изключи този режим (за всички входове) или ако е включен – за всеки вход индивидуално да се определи посоката на свързване на „резистора“.

Зададените стойности стават без значение при задаване на порта като изход.

SNMP: Глобално пускане/спиране на режима: промяна на съответния бит в cfgMode.0 (NO_PULL-UP/DOWN _BIT3)

Индивидуална посока за всеки вход: Промяна на съответния бит в cfgP3Pull.0 и cfgP5Pull.0 (1=Pull-down, 0=Pull-up.)

Web: Меню „Setup-> Pull-up/down for inputs” и таблицата „I/O ports settings“

7.3 Запазване състоянието на изходните I/O портове след рестарт

Стандартно PicoIP инициализира в лог. 0 (ниско ниво) всички изходни портове след подаване на захранващото напрежение или рестарт.

С разрешаването на тази опция, ***PicoIP*** ще съхранява в енергонезависима памет текущото състояние на изходните портове. При рестартиране на PicoIP (или включването му) ще се заредят последните съхранени стойности на изходните портове. Записът на текущото състояние се извършва при всяко подаване на команда за промяна през Web или SNMP. Генерираното от AnalogEvents не се записва!

SNMP: Промяна на съответния бит в cfgNewMode.0
Web: Меню „Setup-> Save I/O ports’ states”

Енергонезависимата памет, която съхранява тази информация се характеризира с ограничен брой презаписи. За това не е удачно този режим да се използва при голяма честота на промяна на състоянията на изходите.

Обновяването на системния софтуер през TFTP води до заличаване на информацията за последното състояние на изходните портове. След обновяването портовете ще имат записана информация за състояние лог. 0. Поради аналогични причини, запазването на състоянието на портовете не се извършва по време на активна TFTP сесия.

©2008-2012, НЕОМОНТАНА ЕЛЕКТРОНИКС

7.4 Цифров филтър на аналоговите входове (P6)

От версия 4.084 в ***PicoIP*** е реализиран цифров филтър върху измерванията през аналоговите входове. За сметка на по-дългото време на конвертиране преди да се върне резултата се постига ефективно изчистване на шумовете от аналоговите входове. Филтърът е включен по подразбиране, но може да бъде деактивиран при необходимост.

SNMP: Промяна на бит (DISABLE_ANALOG_FILTER) в cfgMode.0
Web: Меню „Setup-> Digital filter for ADC ”

7.5 Достъп до I/O през SNMP

За достъп до I/O портовете са заделени три коренни OID-овете: pctrlPort3, pctrlPort5 и pctrlPort6. В тях са дефинирани отделни OID-ове за достъп до отделните пинове (например pctrlPort3.pctrlP3pin1.0), както и за достъп до целия порт като 8 битова единица (pctrlPort3.pctrlP3byte.0). При P6 реално се извършва аналогово измерване на състоянието и конвертиране до цифрови нива (лог.”0” при <1.65V и лог.”1” при >1.65V) и след това се формира pctrlP6byte.0.

При P6 достъпът до определен пин връща като стойност не логическото състояние, а стойността на АЦП за пина (в интервала 0 ... 1023). Аналоговото напрежение на пина може да се определи по формулата:

$$U_{ADC} = 3{,}3.\frac{SNMP_{value}}{1023}[V]$$

За запазване на съвместимостта с аналоговите входове на ***TinyIP*** е запазен достъпа до OID-овете cfgADC3, cfgADC5 и cfgADC7. Тяхното изчитане ще връща същия резултат както при ***TinyIP*** при подаване на същото аналогов напрежение на съответния вход (виж Таблица 3) на ***PicoIP***. За целта измерването от ***PicoIP*** се конвертира до 12bit и се приравнява към 1.5V опорно напрежение – за повече информация вижте 3.2.5.

В допълнение, също с цел съвместимост с ***TinyIP***, е запазен достъпа до root OID-овете pctrlPort3.0, pctrlPort5.0 и pctrlPort6.0. При четене от тях се изчитат съответни входни пинове от P6 (виж 3.2.4).

Тъй-като I/O каналите си групирани в няколко порта за да изчетете абсолютно всички портове ще са необходими няколко 'snmpget' заявки (общо 11 на брой). За да се улесни и ускори извличането на данните от всички обекти е създаден специален OID – pctrlAllPorts.0, който позволява изчитането на всички входно-изходни вериги с една заявка. Този OID връща като резултат OCTET STRING от вида:
"0x40,0x80,0x00,0x0055,0x00BD,0x00AA,0x008D,0x005C,0x0045,0x003E,0x0049".

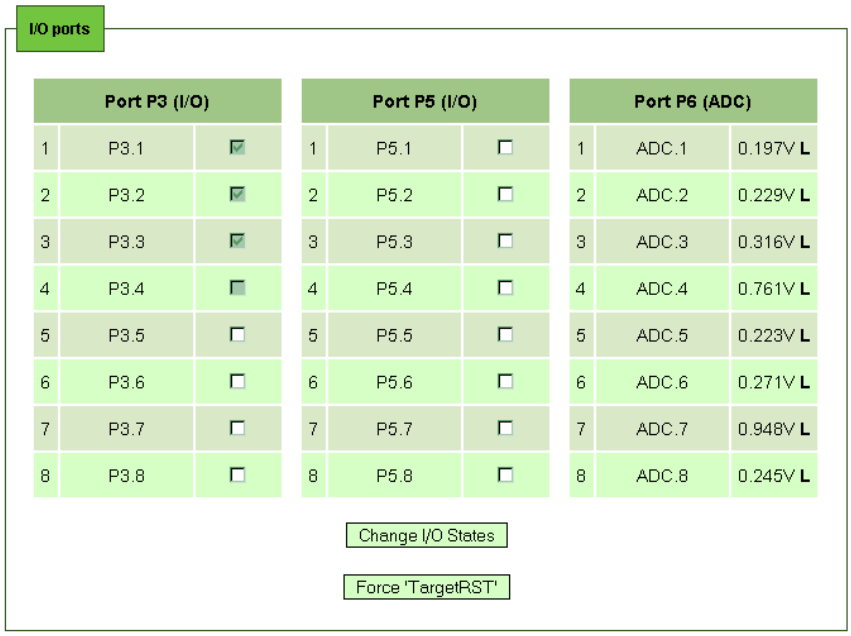
Данните са в шестнадесетичен формат (HEX), поради което са с фиксирана дължина и са подредени както следва:

„P3(8bit),P5(8bit),P6(8bit), P6.1(10bit), P6.2, P6.3, P6.4, P6.5, P6.6, P6.7, P6.8”

©2008-2012, НЕОМОНТАНА ЕЛЕКТРОНИКС

7.6 Достъп до I/O през Web

Изчитането и промяната на I/O портовете през Web е в менюто „I/O ports



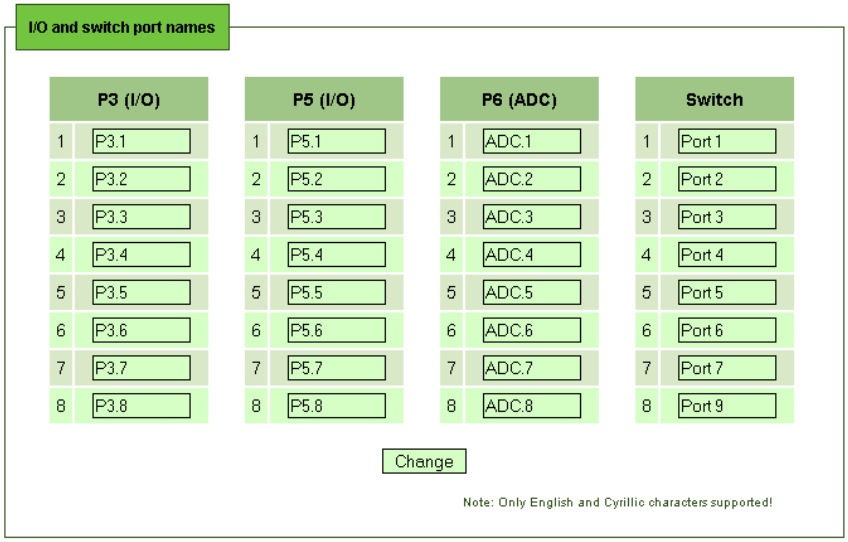
©2008-2012, НЕОМОНТАНА ЕЛЕКТРОНИКС

8. Именуване на I/O и суитч портовете

От версия 4.084 в ***PicoIP*** на потребителя се предоставя възможност да именува всеки един от I/O портовете – общо 24 на брой, както и 8-те порта на SmartSwitch.

Това може да стане само през WEB интерфейса от менюто „Port Labels”. Максималния брой символи за всяко е име е ограничен на 8. Поддържат се English и Cyrllic (Windows-1251) символи.

Всяко обновяване към версия 4.084 ще зарежда фабричните стойности на имената:



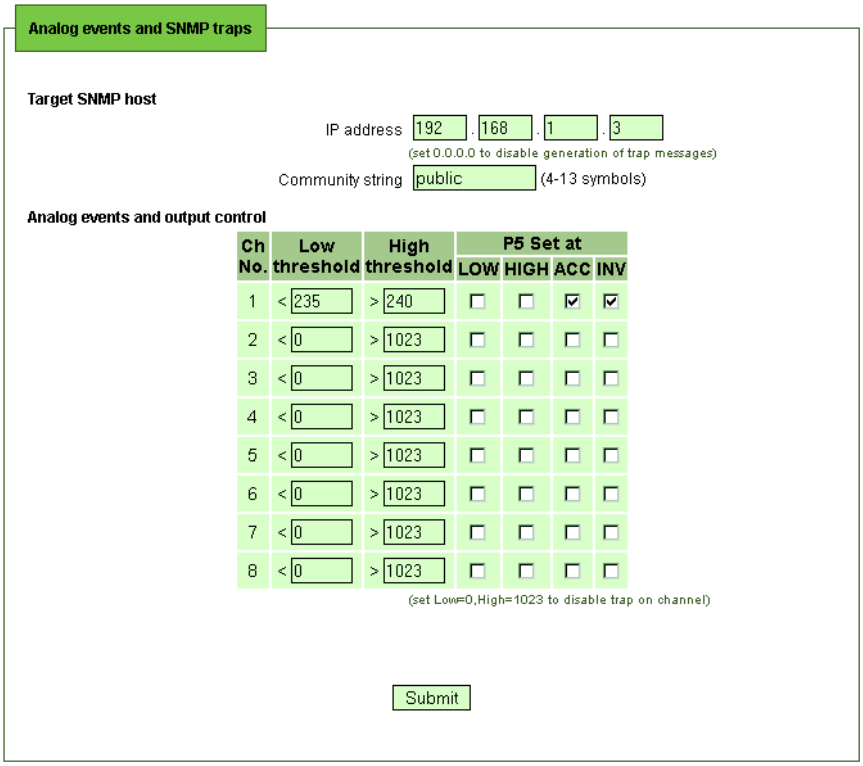
©2008-2012, НЕОМОНТАНА ЕЛЕКТРОНИКС

9. Генериране на събития от аналоговите входове

9.1 SNMP traps

Настройките за SNMP traps са поместени в Web менюто „SNMP traps". ***PicoIP*** може да генерира SNMPv1 traps при следните случаи:

1. рестартиране на ***PicoIP*** - „Cold Start Trap"
2. промяна на линка на порт на суитч (ако е разрешено управление на суитч) – "LinkUp/LinkDown Trap" със „Specific Trap Code" съответстващ на номера на порта
3. промяна на аналогов вход извън зададените граници. Задаването на граници 0 и 1023 е равносилно на спиране на генериране на trap съобщения от даден вход. Съобщението носи като информация OID-а на съответния пин (например. pctrlPort6.pctrlP6pin1) и съответната стойност на АЦП, която е довела до възникването на събитието.



Глобалното спиране на генерирането на всички видове SNMPtraps става чрез задаване като IP адрес 0.0.0.0

Параметрите в Web страницата са достъпни за задаване и през SNMP. За повече информация се обърнете към MIB файла към PicoIP.

*При възникване на няколко едновременни събития за SNMP traps **PicoIP** ги изпраща в реда на тяхното отчитане през интервал от 1-2 секунди.*

За първите два типа събития се изпраща едно единствено trap съобщение при настъпване на събитието. Механизмът на SNMPtraps не гарантира получаването на събитието в target host!

При настъпване на събитие от аналогов вход SNMPtrap съобщение ще се изпраща през 1-2s до възстановяване на аналоговото напрежение в зададения интервал.

©2008-2012, НЕОМОНТАНА ЕЛЕКТРОНИКС

9.2 Генериране на изходни събития (Analog Events)

*Функцията е въведена от версия 4.078 на системния софтуер на **PicoIP**.*

Тази нова функция е изключително полезна в случаите на използване на PicoIP за мониторинг на различни входни величини (аналогови и цифрови). Чрез „Analog Events“ ***PicoIP*** може да се превърне в контролер на процеси, тъй-като вече може да генерира изходни сигнали при определени събития на входовете. Като порт за реакция се използва изцяло изходният порт P5, като пиновете му съответстват на входните сигнали на P6 (аналогово/цифровият вход). Достъпни са три режима на работа:

1) Режим „Low“ - съответният изход се установява в лог. „1“ при спадане на аналоговото входно напрежение под зададения долен праг (Low Threshold) и възстановява в изходно състояние при възстановяване на нивото над прага;

2) Режим „High“ - изходът се установява при надвишаване на зададения горен праг (High Threshold);

3) Режим „Low/High“ - изходът се установява, когато входът е извън обхвата, зададен с долен и горен праг;

4) Режим „Acc“ - в този т.нар. „акумулаторен/хистерезисен“ режим изходът се установява при спадане на напрежението под долния праг и се възстановява при преминаване на горния праг. В този режим лесно може да се реализира автоматично зареждане на акумулатори. Също така може да се използва за включване на товар при спадане на температурата под определен праг и изключване при връщането и над определено ниво (при включен температурен датчик на съответния аналогов вход).

Допълнително е достъпна (от в. 4.097) и опцията „INV” (Инвертиране)– тя обръща нивото на сигнала, който се генерира към P5 (ако стандартно е било да се установи в „1“ при INV се установява в „0“. За примера с температурен датчик – тази опция позволява да се реализира автоматично включване на товар при преминаване на температурата над прага High (изключване при спадането и под прага Low). Обратно (без INV) може да се реализира подгряване при ниски температури (например на антени) – изходът се включва при спадане под LOW и се изключва при повишаване над HIGH.

Функцията не влияе на генерирането на SNMP traps, но използва същите стойности за долен и горен праг на аналоговата стойност.

SNMP: Промяна на стойността в съответния aevPinX.0. Възможните стойности са None, Low, High, LowHigh, Acc

Web: Меню „SNMP traps-> P5 set at”

Достъпът до P5 по стандартния начин (чрез I/O ports в Web или SNMP) функционира дори и когато се използва някой от описаните режими на „Analog Events“.

Опцията „Save I/O ports' states“ също функционира при „Analog Events“, но самите аналогови събития не водят до запис на състоянието на P5 в енергонезависимата памет. Записът се осъществява само при директен достъп до I/O портовете.

©2008-2012, НЕОМОНТАНА ЕЛЕКТРОНИКС

10. Фабрични настройки

10.1 Фабрични стойности на параметрите на *PicoIP*

Тук са поместени всички параметри на ***PicoIP*** с техните стойности, заложени при производството на ***PicoIP***.

Таблица 4 Списък на фабричните стойности

Параметър (според означенията на Web страниците)	**Стойност**
DHCP	Disabled
IP	172.16.100.2
Mask	255.255.255.0
Gateway	172.16.100.1
VLAN ID	1
VLAN mode	Disabled
Access MAC1,2	000000000000
SNMP access to IP	Enabled
SNMP listen UDP port	161
SNMP Read-only string	000000000000
SNMP RW string	private
SNMP/Web Access network IP	172.16.100.1
SNMP/Web Access network Mask	0.0.0.0 (disabled)
Ping Timeout	6
Number of Restarts	255 (unlimited)
RestartSwitch	Enabled
RestartExternal Device	Enabled
External Pulse Width	100 (x250ms)
Restart on incoming ping timeout	Disabled
Restart on remote IP timeout	Disabled
Remote IP to ping	172.16.100.1
I/O ports settings	P3,P5 - Outputs
Pull-Up/Pull-Down	All “pull-down”
Pull-up/down for inputs	Enabled
Duplicate 'TargetRST' on P5	Off for all pins
Reset I/O ports on restart	Disabled
Digital filter for ADC	Enabled
Toggle JP6.4 on outgoing ping request (Ping LED)	Disabled
Second LED mode	'Power ON'
TFTP update	Enabled
TFTP Server IP	172.16.100.1
Switch Control	Disabled
Broadcast Frames	Parse
Web Server	Enabled
Web Server TCP port	80
SNMP traps target host	172.16.100.1
SNMP traps community	public
Low/High Analog Trap Threshold	0/1023 (disabled)
Analog Events – Low, High, Acc	None
Web user/password	admin/admin

©2008-2012, НЕОМОНТАНА ЕЛЕКТРОНИКС

10.2 Зареждане на фабричните настройки в *PicoIP*

В случай на неправилно конфигуриране на ***PicoIP*** е възможно да се загуби достъпа до него. Единственото сигурно решение в този случай е да се направи зареждане на всички негови настройки с фабричните такива. За целта е предвиден джъмпер “Reset to Default” (виж 11): подайте захранване на ***PicoIP*** (или го рестартирайте с команда) при поставен джъмпер; това веднага ще доведе до стартиране с фабричните настройки. Премахнете джъмпера!!!

В ***PicoIP*** версия 4.094 и по-нови – зареждането на фабричните настройки се съпровожда с няколкократно премигване на вторият LED.

При версии по-стари от 4.077 (включително) възстановяването на фабричните настройки не се възприема мигновено. Необходимо повторно изключване/включване на захранването на модула за да се инициализира с фабричните настройки.

За джъмпер ДА НЕ СЕ ИЗПОЛЗВА наличният на платката друг единичен и фабрично поставен джъмпер!

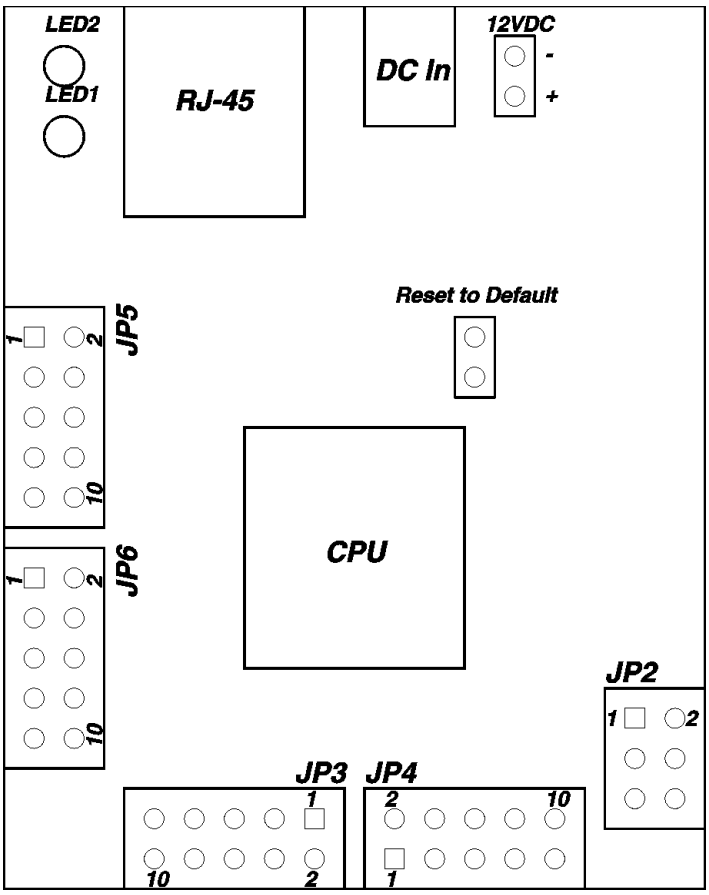
Ако PicoIP е в режим „Switch Control” поставянето на джъмпера ще доведе до опит за нулиране към фабрични настройки и на суитча!

От версия 4.097 е предвидена и „софтуерна“ възможност за зареждане на фабричните настройки. Това може да стане през WEB интерфейса или през SNMP. Изпълнението на тези команди води до последващо рестартиране на PicoIP. Ако към PicoIP има включен суитч – неговите настройки НЕ СЕ НУЛИРАТ при тези команди.

SNMP: Изчитане на cfgDefault.0
Web: Меню „IP Core → Default”

©2008-2012, НЕОМОНТАНА ЕЛЕКТРОНИКС

11. ПРИЛОЖЕНИЕ 1 Разположение и значение на I/O портове на *PicoIP* хардуерна версия 1.2.



Изводите не са буферирани/защитени и са директно свързани с CPU.

Максималният ток на изходните изводи е 1мА, като нивата са при 3.3V логика.

На входните изводи трябва да се подава напрежение от 0 до 3.3V; или да е токоограничено спрямо 3.3 волтова логика на 0.25мА;

Конекторът с 12VDC е свързан през диод към входния жак. При подаването на захранване през него трябва обезателно да се спазва правилния поляритет. Подаденото на него захранване няма да „излезе“ жака!

Таблица 5 Описание на I/O портовете, заделени за свободен достъп от потребителя

	Port P3 (JP3) /цифров I/O/			**Port P5** (JP4) /цифров I/O/			**Port P6** (JP5) /изцяло входен, аналогов и цифров/		
PIN No.	Bit	FUNC	DIR	Bit	FUNC	DIR	Bit	FUNC	DIR
1	1	Free	I/O	1	Free	I/O	1	Free	Ain
2	2	Free	I/O	2	Free	I/O	2	Free	Ain
3	3	Free	I/O	3	Free	I/O	3	Free	Ain
4	4	Free	I/O	4	Free	I/O	4	Free	Ain
5	5	Free	I/O	5	Free	I/O	5	Free	Ain
6	6	Free	I/O	6	Free	I/O	6	Free	Ain
7	7	Free	I/O	7	Free	I/O	7	Free	Ain
8	8	Free	I/O	8	Free	I/O	8	Free	Ain
9	-	GND	PWR	-	+3.3V	PWR	-	+3.3V(Vref)	PWR
10	-	GND	PWR	-	GND	PWR	-	GND	PWR

Таблица 6 Описание на системния порт (недостъпен директно)

	Port JP6 /системен порт/		
PIN No.	Bit	FUNC	DIR
1	-	+3.3V	PWR
2	-	+3.3V	PWR
3	-	Reserved	-
4	-	Ping LED	Out
5	-	Reserved	-
6	-	Target RST	Out
7	-	Switch (RST)	Out
8	-	Switch (SCL)	Out
9	-	Switch (SDA)	In/Out
10	-	GND	PWR

Легенда:

“Free” – изводът е свободен за използване от потребителя;

“*XXXXXX*” – изводът е заделен за определена системна функция

“In” – изводът е вход, „Out” – изход, „I/O – вход или изход според настройките

“Ain” – аналогов вход

©2008-2012, НЕОМОНТАНА ЕЛЕКТРОНИКС

12. ПРИЛОЖЕНИЕ 2 Захранване на модула и интерфейс на I/O портовете

12.1 Захранване на модула.

Минималното захранващо напрежение на модула е **7.5VDC**.

Максималното напрежение е **25VDC** и е ограничено единствено от входния филтриращ кондензатор (теоретично импулсният конвертор може да работи до 40VDC). Оптималното захранващо напрежение е около **12VDC**. Консумираната мощност не зависи от входното напрежение и е около **0.55W** (46mA@12V).

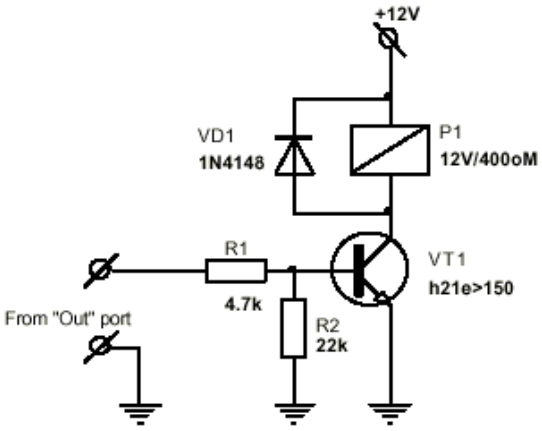
От хардуерна версия 1.2 на PicoIP (след 01.04.2011) той е снабден със защита от обратно включване!

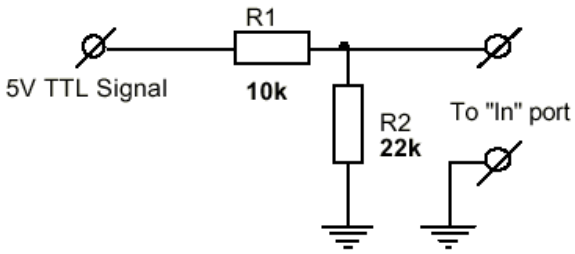
Хардуерни версии по-стари от 1.2 на PicoIP нямат защита срещу погрешен поляритет на захранващото напрежение!!!Обръщането на поляритета, както и подаването на променливо напрежение ще доведе до повреда!!!

12.2 Външно свързване I/O портовете.

Те са директно изведени от микроконтролера и не са буферирани, поради което трябва внимателно да се работи с тях за да не се повреди MCU. Те са цифрови изходи/входове, като изходното има напрежение при лог. “1” е 3.3V, а при лог. “0” под 0.25V при консумация <1.5мА. Всички входове/изходи имат защитни диоди спрямо маса и +Vcc (3.3V).

По долу са дадени примерни схеми на свързване на I/O портовете към външни устройства. На първата е показана примерна схема за управление на стандартно външно реле за 12V. На втората – примерно съгласуване към външен 5V TTL сигнал. По принцип резисторът R2 не е задължителен, но е препоръчителен, особено когато се работи с външни сигнали, които заемат и “tri-state” (плаващо) състояние.





По първата схема са реализирани и модулите „Relay Board” и “RelayBox2x”, който е специално разработен за ***PicoIP*** и дава възможност за управление на 4 или 2 канала с релета за 7A/ 220VAC.

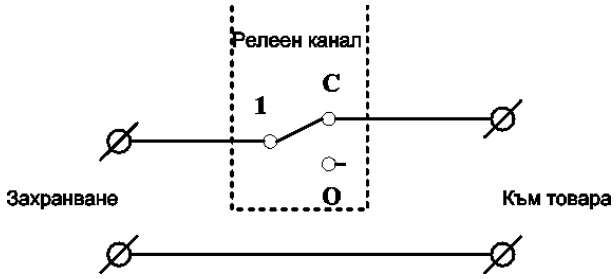
©2008-2012, НЕОМОНТАНА ЕЛЕКТРОНИКС

13. ПРИЛОЖЕНИЕ 3 Свързване на *PicoIP* към разширителните модули *RelayBox2x* и *RelayBoard.*

Неомонтана Електроникс предлага два разширителни модула с релейни изходи на базата на концепцията описана в 12.2.

Модулите позволяват управлението на два (*RelayBox2x*) или четири (*RelayBoard*) мощни консуматора (до 7A/240VAC) чрез маломощните изходни портове на ***PicoIP***. Комутирането на товара става посредством превключващ контакт на релетата - при подаване на входен сигнал релето включва и контактната му система застава в положение "NO" - нормално отворено.

В практиката, най-често се налага рестартиране (прекъсване на нормално затворена верига) на захранването на някакъв тип мрежово обурудване. За целта е необходимо да се използва нормално затворения контакт на комутатора, през който се провежда единия от захранващите проводници. Така, при липса на сигнал от ***PicoIP*** веригата е затворена и товарът има постоянно захранване. При команда (автоматична или ръчна) оборудването се рестартира поради прекъсване на захранването му.



Тъй-като ***PicoIP*** разполага с 16 изходни порта, то свободно могат да се комбинират съответния брой 2- и 4-канални комутатори с цел постигане на желания брой вериги за управление.

За свързване към ***PicoIP*** е необходимо първо да се свърже общият проводник ("-", черен цвят) към някои от свободните "GND" изводи на ***PicoIP*** (виж 11). Входовете на каналите се свързват към някои от свободните изводи на ***PicoIP***, които са означени като изходи ("Out") – това се целият P3, P5 и JP6.6 (TargetRST). Изходите е необходимо и да бъдат конфигурирани като изходи. Необходимо е и да се захрани комутатора с 12VDC (най-добре да се разклони захранването на ***PicoIP)*** .

Възможни са следните два режима на управление на консуматорите, в зависимост от използвания изход на ***PicoIP***.

13.1 "Рестартиращо" управление

В този режим входа на даден канал на релейните комутатори трябва да е свързан към сигнала TargetRST (JP6.6) или към изводи на P5, които са разрешени за „Duplicate 'TargetRST' on P5 pins" (виж 3.2.2).

При подаване на команда "Target Restart" през Web или SNMP, съответния релеен канал се задейства (релето включва) за време от 25s (може да се настройва), след което то автоматично се изключва.

Това рестартиращо управление се задейства и при мониторинг режимите чрез ping ("Ping Timeout Restart", "Remote Ping Restart"). Предимството на този режим е, че връщането в изходно състояние става автоматично, което дава възможност за рестартиране на устройство, през което преминава Ethernet линка към IP модула. Така връзката към модула се възстановява автоматично след рестарта и той продължава да е достъпен през SNMP. При този режим се използват изходните пинове "Sec. RST" или "RST" за TinyIP; "Target RST" при PicoIP.

©2008-2012, НЕОМОНТАНА ЕЛЕКТРОНИКС

13.2 Ръчно управление

При този режим се използват стандартните изходи (общо 16бр.) на ***PicoIP*** – P3 и P5. За включване на съответното реле е необходимо да се постави отметка на съответния бит на порта в WEB или WinTIC или да се подаде необходимата SNMP команда. Изключването на релето става ръчно след махане на отметката.

Прекъсването на линка към IP модула след включване/изключване на някое реле ще доведе до невъзможност за връщане на релето в изходно състояние. За това внимателно да се преценява топологията на управлението и ако е необходимо да се използва "рестартиращо" управление.

©2008-2012, НЕОМОНТАНА ЕЛЕКТРОНИКС

14. ПРИЛОЖЕНИЕ 4 Бързо ръководство за работа с SNMP

SNMP протокола дефинира отделни обекти във всяко устройство, които могат да се изчитат или записват според типа им. Тези обекти има т.нар. OID – (object id), който ги характеризира еднозначно. Въпросните обекти се описват на специален синтаксис в текстов файл (MIB файл), който позволява вместо трудните за запомняне цифрови еквиваленти на OID-овете да се ползват имена.

OID-овете представляват дървовидна структура от типа .1.2.3.4.5..... и така се формира уникален номер за всеки обект. Тази структура е описани в съответния MIB файл. Неомонтана Електроникс има регистриран „клон“ в тази структура, който е **1.3.6.1.4.1.19865.**

За достъп до параметрите на PicoIP се използват командите snmget и snmpset. Синтаксисът е аналогичен:

>snmpget -v1 -c <парола read-only> <IP> <OID>

>snmpset -v1 -c <парола read-write> <IP> <OID> <тип данни> <стойност>

Командата snmpset изисква точното указване на типа данни, които ще се подадат на съответния OID. Допустимите типове са:

i: INTEGER, u: unsigned INTEGER, t: TIMETICKS, a: IPADDRESS
o: OBJID, s: STRING, x: HEX STRING, d: DECIMAL STRING, b: BITS
U: unsigned int64, I: signed int64, F: float, D: double

За изчитане на IP адреса се използва:

> snmpget -v1 -c 000000000000 172.16.100.2 cfgIP.0

или (ако SNMP клиента не е правилно конфигуриран да зарежда MIB фйла)

> snmpget -v1 -m c:/usr5/share/snmp/mibs/picoIP-MIB.txt -c 000000000000 172.16.100.2 cfgIP.0

Винаги може да се използва цифровия еквивалент на всеки OID. Този вариант е универсален и ще работи винаги при всякакви SNMP клиенти:

>snmpget -v1 -c 000000000000 172.16.100.2 **1.3.6.1.4.1.19865.1.1.1.0**

В „превод“ цифровият еквивалент означава:

(1.3.6.1.4.1.19865)	.1	.1	.1	.0
Neomontana	.PicoIP	. Configuration	. CfgIP	. 0

Други примерни команди:

- задаване на нивото на изход P3.1
  > snmpset -v1 -c private 172.16.100.2 pctrlP3pin1.0 i High
  или
  > snmpset -v1 -c private 172.16.100.2 1.3.6.1.4.1.19865.1.2.1.1.0 i 1
- задаване на нов IP адрес
  > snmpset -v1 -c private 172.16.100.2 cfgIP.0 a 172.16.100.50
- рестартиране на „TargetRST”
  snmpget -v1 -c 000000000000 172.16.100.2 pctrlRestart.0
  или
  snmpget -v1 -c 000000000000 172.16.100.2 1.3.6.1.4.1.19865.1.2.4.0

По долу е поместени резултата от командата 'snmptranslate', която съставя дървовидна структура с имената и номерата на обектите и подобектите. От нея лесно може да се извлече цифровият еквивалент на всеки обект като се премине по разклоненията на дървото. От дървото добре се вижда и типа данни които ще изисква при запис всеки обект, както и дали е само за четене или за четене/запис.

```
>snmptranslate -Tp -IR -Ov Neomontana
+--Neomontana(19865)
   |
   +--TinyIP(1)
   | |
   | +--Configuration(1)
   | | |
   | | +-- -RW- IpAddr    cfgIP(1)
   | | +-- -R-- String    cfgMAC(2)
   | | |       Textual Convention: PhysAddress
   | | |       Size: 6
   | | +-- -RW- INTEGER   cfgVLANTag(3)
   | | |       Range: 0..4095
   | | +-- -RW- String    cfgPassword(4)
   | | |       Size: 4..12
   | | +-- -RW- String    cfgMACLock1(5)
   | | |       Textual Convention: PhysAddress
   | | |       Size: 6
   | | +-- -RW- String    cfgMACLock2(6)
   | | |       Textual Convention: PhysAddress
   | | |       Size: 6
   | | +-- -RW- INTEGER   cfgPingTime(7)
   | | |       Range: 0..255
   | | +-- -R-- INTEGER   cfgVersion(8)
   | | |       Range: 0..65535
   | | +-- -RW- INTEGER   cfgMode(9)
```

©2008-2012, НЕОМОНТАНА ЕЛЕКТРОНИКС

```
| | |       Range: 0..255
| | +-- -R-- Null      cfgReset(10)
| | +-- -RW- INTEGER   cfgNewMode(11)
| | |       Range: 0..255
| | +-- -RW- INTEGER   cfgResetPulse(12)
| | |       Range: 0..32767
| | +-- -RW- INTEGER   cfgResetCount(13)
| | |       Range: 0..255
| | +-- -RW- IpAddr    cfgDefGW(14)
| | +-- -RW- IpAddr    cfgNetMask(15)
| | +-- -RW- IpAddr    cfgMonitorIP(16)
| | +-- -RW- String    cfgReadOnlyPassword(17)
| | |       Size: 4..12
| | +-- -RW- IpAddr    cfgTrapServerIP(18)
| | +-- -RW- String    cfgTrapPassword(19)
| | |       Size: 4..12
| | +-- -RW- IpAddr    cfgAccessIP(20)
| | +-- -RW- IpAddr    cfgAccessMask(21)
| | +-- -RW- INTEGER   cfgHTTPport(22)
| | |       Range: 0..65535
| | +-- -RW- INTEGER   cfgSNMPport(23)
| | |       Range: 0..65535
| | +-- -RW- EnumVal   cfgLED2mode(24)
| | |       Values: PowerOn(0), PingIn(1), PingOut(2), PingBoth(3), ValidIP(4)
| | +-- -RW- INTEGER   cfgP3Dir(25)
| | |       Range: 0..255
| | +-- -RW- INTEGER   cfgP5Dir(26)
| | |       Range: 0..255
| | +-- -RW- INTEGER   cfgP3Pull(27)
| | |       Range: 0..255
| | +-- -RW- INTEGER   cfgP5Pull(28)
| | |       Range: 0..255
| | +-- -RW- INTEGER   cfgP5DupRST(29)
| | |       Range: 0..255
| | +-- -R-- Null      cfgDefault(30)
| | +-- -RW- IpAddr    cfgTFTPServerIP(32)
| | +-- -R-- Null      cfgUpdateFirmware(33)
| | |
| | +--AnalogEvent(121)
| | | |
| | | +-- -RW- EnumVal   aevPin1(1)
| | | |       Values: None(0), Low(1), High(2), LowHigh(3), Acc(4)
| | | +-- -RW- EnumVal   aevPin2(2)
| | | |       Values: None(0), Low(1), High(2), LowHigh(3), Acc(4)
| | | +-- -RW- EnumVal   aevPin3(3)
| | | |       Values: None(0), Low(1), High(2), LowHigh(3), Acc(4)
| | | +-- -RW- EnumVal   aevPin4(4)
| | | |       Values: None(0), Low(1), High(2), LowHigh(3), Acc(4)
| | | +-- -RW- EnumVal   aevPin5(5)
| | | |       Values: None(0), Low(1), High(2), LowHigh(3), Acc(4)
| | | +-- -RW- EnumVal   aevPin6(6)
| | | |       Values: None(0), Low(1), High(2), LowHigh(3), Acc(4)
| | | +-- -RW- EnumVal   aevPin7(7)
| | | |       Values: None(0), Low(1), High(2), LowHigh(3), Acc(4)
| | | +-- -RW- EnumVal   aevPin8(8)
| | | |       Values: None(0), Low(1), High(2), LowHigh(3), Acc(4)
| | | +-- -RW- EnumVal   aevPin1Inv(9)
| | | |       Values: None(0), Inverted(1)
| | | +-- -RW- EnumVal   aevPin2Inv(10)
| | | |       Values: None(0), Inverted(1)
| | | +-- -RW- EnumVal   aevPin3Inv(11)
| | | |       Values: None(0), Inverted(1)
| | | +-- -RW- EnumVal   aevPin4Inv(12)
| | | |       Values: None(0), Inverted(1)
| | | +-- -RW- EnumVal   aevPin5Inv(13)
| | | |       Values: None(0), Inverted(1)
| | | +-- -RW- EnumVal   aevPin6Inv(14)
| | | |       Values: None(0), Inverted(1)
| | | +-- -RW- EnumVal   aevPin7Inv(15)
| | | |       Values: None(0), Inverted(1)
| | | +-- -RW- EnumVal   aevPin8Inv(16)
| | | |       Values: None(0), Inverted(1)
| | | |
| | +--AnalogTrap(122)
| | | |
| | | +-- -RW- INTEGER   atrPin1Low(1)
| | | |       Range: 0..1023
| | | +-- -RW- INTEGER   atrPin1High(2)
| | | |       Range: 0..1023
| | | +-- -RW- INTEGER   atrPin2Low(3)
| | | |       Range: 0..1023
| | | +-- -RW- INTEGER   atrPin2High(4)
| | | |       Range: 0..1023
| | | +-- -RW- INTEGER   atrPin3Low(5)
| | | |       Range: 0..1023
| | | +-- -RW- INTEGER   atrPin3High(6)
| | | |       Range: 0..1023
| | | +-- -RW- INTEGER   atrPin4Low(7)
| | | |       Range: 0..1023
| | | +-- -RW- INTEGER   atrPin4High(8)
| | | |       Range: 0..1023
| | | +-- -RW- INTEGER   atrPin5Low(9)
| | | |       Range: 0..1023
| | | +-- -RW- INTEGER   atrPin5High(10)
| | | |       Range: 0..1023
| | | +-- -RW- INTEGER   atrPin6Low(11)
| | | |       Range: 0..1023
| | | +-- -RW- INTEGER   atrPin6High(12)
| | | |       Range: 0..1023
| | | +-- -RW- INTEGER   atrPin7Low(13)
| | | |       Range: 0..1023
| | | +-- -RW- INTEGER   atrPin7High(14)
| | | |       Range: 0..1023
| | | +-- -RW- INTEGER   atrPin8Low(15)
| | | |       Range: 0..1023
| | | +-- -RW- INTEGER   atrPin8High(16)
| | | |       Range: 0..1023
| | | |
| | | +-- -R-- INTEGER   cfgADC3(123)
| | | |       Range: 0..65535
| | | +-- -R-- INTEGER   cfgADC5(124)
| | | |       Range: 0..65535
| | | +-- -R-- INTEGER   cfgADC7(125)
| | | |       Range: 0..65535
| | | +-- -R-- INTEGER   cfgTemperature(127)
| | | |       Range: 0..65535
| | | |
| | +--PortCTRL(2)
| | | |
| | | +-- -RW- INTEGER   pctrlPort3(1)
| | | |       Range: 0..255
| | | | +-- -RW- EnumVal   pctrlP3pin1(1)
| | | | |       Values: High(1), Low(0)
| | | | +-- -RW- EnumVal   pctrlP3pin2(2)
| | | | |       Values: High(1), Low(0)
| | | | +-- -RW- EnumVal   pctrlP3pin3(3)
| | | | |       Values: High(1), Low(0)
| | | | +-- -RW- EnumVal   pctrlP3pin4(4)
| | | | |       Values: High(1), Low(0)
| | | | +-- -RW- EnumVal   pctrlP3pin5(5)
| | | | |       Values: High(1), Low(0)
| | | | +-- -RW- EnumVal   pctrlP3pin6(6)
| | | | |       Values: High(1), Low(0)
| | | | +-- -RW- EnumVal   pctrlP3pin7(7)
| | | | |       Values: High(1), Low(0)
| | | | +-- -RW- EnumVal   pctrlP3pin8(8)
| | | | |       Values: High(1), Low(0)
| | | | +-- -RW- INTEGER   pctrlP3byte(33)
| | | |         Range: 0..255
| | | |
| | | +-- -RW- INTEGER   pctrlPort5(2)
| | | |       Range: 0..255
| | | | +-- -RW- EnumVal   pctrlP5pin1(1)
| | | | |       Values: High(1), Low(0)
| | | | +-- -RW- EnumVal   pctrlP5pin2(2)
| | | | |       Values: High(1), Low(0)
| | | | +-- -RW- EnumVal   pctrlP5pin3(3)
| | | | |       Values: High(1), Low(0)
| | | | +-- -RW- EnumVal   pctrlP5pin4(4)
| | | | |       Values: High(1), Low(0)
| | | | +-- -RW- EnumVal   pctrlP5pin5(5)
| | | | |       Values: High(1), Low(0)
| | | | +-- -RW- EnumVal   pctrlP5pin6(6)
| | | | |       Values: High(1), Low(0)
| | | | +-- -RW- EnumVal   pctrlP5pin7(7)
| | | | |       Values: High(1), Low(0)
| | | | +-- -RW- EnumVal   pctrlP5pin8(8)
| | | | |       Values: High(1), Low(0)
| | | | +-- -RW- INTEGER   pctrlP5byte(33)
| | | |         Range: 0..255
| | | |
| | | +-- -RW- INTEGER   pctrlPort6(3)
| | | |       Range: 0..255
| | | | +-- -R-- INTEGER   pctrlP6pin1(1)
| | | | |       Range: 0..1023
| | | | +-- -R-- INTEGER   pctrlP6pin2(2)
| | | | |       Range: 0..1023
| | | | +-- -R-- INTEGER   pctrlP6pin3(3)
| | | | |       Range: 0..1023
| | | | +-- -R-- INTEGER   pctrlP6pin4(4)
| | | | |       Range: 0..1023
| | | | +-- -R-- INTEGER   pctrlP6pin5(5)
| | | | |       Range: 0..1023
| | | | +-- -R-- INTEGER   pctrlP6pin6(6)
| | | | |       Range: 0..1023
| | | | +-- -R-- INTEGER   pctrlP6pin7(7)
| | | | |       Range: 0..1023
| | | | +-- -R-- INTEGER   pctrlP6pin8(8)
| | | | |       Range: 0..1023
| | | | +-- -RW- INTEGER   pctrlP6byte(33)
| | | |         Range: 0..255
| | | |
| | | +-- -R-- Null      pctrlRestart(4)
| | |
| | | +-- -R-- String    pctrlAllPorts(5)
| | |
| | +--Switch(3)
| | |
| | +--RTL8309SBCTRL(4)
| | | |
| | | +-- -R-- Null      rtlRestart(1)
| | | |
| | | +--rtlEEPROM(2)
| | | | |
| | | | +-- -RW- INTEGER   rtlEEx00(0)
| | | | |       Range: 0..255
| | | | +-- -RW- INTEGER   rtlE0x01(1)
| | | | |       Range: 0..255
| | | | +-- -RW- INTEGER   rtlE0x7F(127)
| | | |         Range: 0..255
| | | |
| | | +--rtlPHY(3)
| | | | |
| | | | +-- -RW- INTEGER   rtlPHYx00(0)
| | | | |       Range: 0..65535
| | | | +-- -RW- INTEGER   rtlPHYxFF(255)
| | | |         Range: 0..65535
| | | |
| | | +-- -R-- Null      rtlApply(4)
| |
| +--PicoIP(1)
```

©2008-2012, НЕОМОНТАНА ЕЛЕКТРОНИКС