



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY



**FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH
TECHNOLOGIÍ**

ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
DEPARTMENT OF TELECOMMUNICATIONS

NASAZENÍ PRVKŮ ATEN PRO DÁLKOVÝ DOHLED NAD SÍŤOVÝMI UZLY

DEPLOYMENT OF ATEN ELEMENTS FOR REMOTE MANAGEMENT OF NETWORK NODES

BAKALÁŘSKÁ PRÁCE

BACHELOR'S THESIS

AUTOR PRÁCE

AUTHOR

DÁVID KONDICZ

VEDOUCÍ PRÁCE

SUPERVISOR

doc. Ing. VÍT NOVOTNÝ, Ph.D.

BRNO 2012



**VYSOKÉ UČENÍ
TECHNICKÉ V BRNĚ**

**Fakulta elektrotechniky
a komunikačních technologií**

Ústav telekomunikací

Bakalářská práce

bakalářský studijní obor
Teleinformatika

Student: Dávid Kondicz

ID: 98223

Ročník: 3

Akademický rok: 2011/2012

NÁZEV TÉMATU:

Nasazení prvků ATEN pro dálkový dohled nad síťovými uzly

POKYNY PRO VYPRACOVÁNÍ:

Prostudujte prostředky dálkového ovládání prvků datových IP sítí. Seznamte se s nástroji ATEN KH-1516i, ATEN SN-0116 a ATEN PN-9108 a navrhnete jejich využití při správě výukové a experimentální datové sítě v laboratoři PA-427. Na základě získaných zkušeností navrhnete laboratorní úlohu.

DOPORUČENÁ LITERATURA:

- [1] SOSINSKY B. Mistrovství - Počítačové sítě. Computer Press, ISBN 9788025133637, ČR, 2010
- [2] ATEN – manuály k produktům ATEN KH-1516i, ATEN SN-0116 a ATEN PN-9108. 2010

Termín zadání: 6.2.2012

Termín odevzdání: 31.5.2012

Vedoucí práce: doc. Ing. Vít Novotný, Ph.D.

Konzultanti bakalářské práce:

prof. Ing. Kamil Vrba, CSc.

Předseda oborové rady

UPOZORNĚNÍ:

Autor bakalářské práce nesmí při vytváření bakalářské práce porušit autorská práva třetích osob, zejména nesmí zasahovat nedovoleným způsobem do cizích autorských práv osobnostních a musí si být plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č.40/2009 Sb.

Prehlásenie

Prehlasujem, že svoju záverečnú bakalársku prácu na tému „Nasazení prvků ATEN pro dálkový dohled nad síťovými uzly“ som vypracoval samostatne, pod vedením vedúceho semestrálnej práce a s použitím odbornej literatúry a ďalších informačných zdrojov, ktoré sú všetky citované v práci a uvedené v zozname literatúry na konci práce.

Ako autor uvedenej semestrálnej práce ďalej prehlasujem, že v súvislosti s vytvorením tejto práce som neporušil autorské práva tretích osôb, najmä som nezasiahol nedovoleným spôsobom do cudzích autorských práv osobnostných a som si plne vedomí následkov porušenia ustanovenia § 11 a nasledujúcich autorského zákona č. 121/2000 Sb., vrátane možných trestnoprávnych dôsledkov vyplývajúcich z ustanovenia § 152 trestného zákona č. 140/1961 Sb.

V Brne dňa

.....
podpis autora

Pod'akovanie

Týmto by som chcel pod'akovať vedúcemu bakalárskej práce doc. Ing. Vítovi Novotnému, PhD., za inšpiratívne rady, veľmi užitočnú metodickú pomoc a odborný dohľad pri spracovaní mojej bakalárskej práce.

V Brne dňa

.....
podpis autora

Anotácia

Predložená práca sa zaoberá problematikou vzdialeného manažmentu a nasadením prvkov diaľkového dohľadu nad sieťovými uzlami so zariadeniami KH-1516i, SN-0116 a PN-9108 od výrobcu ATEN. V práci je uvedená celá škála služieb vhodných pre vzdialený manažment dátového centra od vzdialeného ovládania napájania až po vzdialenú konzolu, náhradu monitora, klávesnice a myši. Sú tu uvedené možnosti integrácie hardvéru so softvérom pre dohľadové centrá. Zo získaných informácií bola vypracovaná laboratórna úloha. V úlohe sa tiež zameriavame na možnosti aplikácie vzdialeného manažmentu rôznych zariadení. Cieľom úlohy bude študentom priblížiť možnosti využitia jednotlivých zariadení v skutočnej prevádzke. Uvedieme aj možnosti redundantného prístupu k jednotlivým dohľadovým zariadeniam.

Kľúčové slová:

KVM Over the NET, Power Over the NET, Serial Over the NET, ATEN, ALTUSEN, Vzdialený manažment siete, RMON

Abstract

The submitted work deals with the problem of setting of long distant sight above network junction with the appliances KH-1516i, SN-0116 and PN-9108 from ATEN manufacturer. We acquaint with the whole spectrum of services suitable for distant management of data centre from distant operating of supply till the distant brace, substitution of monitor, keyboard and mouse. A laboratory task was worked out from information obtained before. We aim at the simulation of application of distant management of switchboard in centre of telecommunication operator with the distant administration of servers. The aim of this task is to bring closer the use possibilities of each appliance in real operating. We also show the possibilities of redundant access to particular supervisory appliances.

Key words:

KVM Over the NET, Power Over the NET, Serial Over the NET, ATEN, ALTUSEN, Distant network management, RMON

Citácia

KONDICZ, D. *Nasazení prvků ATEN pro dálkový dohled nad síťovými uzly*. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2012. 51 s. Vedoucí bakalářské práce doc. Ing. Vít Novotný, Ph.D.

Obsah

Úvod.....	7
1 Možnosti vzdialeného dohľadu.....	8
1.1 Vzdialený dohľad všeobecne.....	8
1.2 Využitie hardvéru pre vzdialený dohľad	8
1.3 Využitie softvéru pre vzdialený dohľad	10
1.4 Dohľadové systémy a dohľadové centrá	13
2 KVM Over the NET	15
3 Serial Over the NET	22
4 Power Over the NET.....	26
4 Výsledok práce na zariadeniach ATEN.....	31
5 Záver	32
Použitá literatúra	34
Zoznam príloh	35
Prílohy.....	36

Úvod

Nočnou morou, už nielen geograficky rozšírených telekomunikačných operátorov je vzdialený manažment a vzdialený dohľad nad uzlami telekomunikačnej siete. Za účelom riešenia tohto problému operátori používajú rôzne systémy a zariadenia, medzi nimi aj KVM prepínače, ktoré predĺžia ruky správcovi siete až na konkrétne zariadenie v sieti. Aplikácia týchto zariadení nielen zjednoduší nastavovanie a správu vzdialených serverov, ale môže nezanedbateľne zlepšiť reakčnú dobu v prípade výpadku niektorého zo zariadení v danom uzle telekomunikačnej siete.

Vzhľadom k tomu, že sa v práci máme zoznámiť a tiež sa máme zaoberať aj so všeobecnou problematikou vzdialeného dohľadu, uvedieme niekoľko zaujímavých a alternatívnych možností, ktoré sa v súčasnosti využívajú. Pozrieme sa do minulosti a uvedieme si aj možnosti praktického využitia jednotlivých technických riešení.

Neraz sa aj mne osobne stalo, že neopatrnosťou som pri konfigurácii prepínača cez SSH odstavil nielen segment siete, ale aj možnosť manažmentu samotného prepínača prostredníctvom IP protokolu. Jedinou možnosťou bola náprava konfigurácie cez sériové rozhranie priamo na mieste, kde bol prepínač umiestnený. Postupné rozširovanie portfólia poskytovaných služieb operátormi, otázky dohľadu ešte viac komplikujú. Okrem dohľadu a správy serverov, prepínačov, alebo smerovačov sú na dohľad niekoľko násobne náročnejšie prvky ústredne digitálnej televízie.

Tvrdý reštart cez napájaciu zásuvku alebo konfigurácia vyžadujúca fyzickú prítomnosť správcu? Na riešenie takýchto a podobných problémov sú ako stvorené zariadenia na vzdialenú správu z rady Over the NET. Tieto zariadenia sú na trhu veľmi rozšírené. Nájdeme ich v ponuke výrobcov ako sú D-LINK, Intellinet, Belkin alebo spoločnosti Aten, ktoré sú aj náplňou tejto práce. Podľa rozsahu určenia môžeme požiť GSM zásuvky, rádiové modemy určené na zber dát zo sériového rozhrania alebo takzvané IP Smart Boardy, ktoré majú na diaľku ovládateľné spínané výstupy a možnosť merania teploty prostredia. Tieto zariadenia nie sú určené výhradne na vzdialenú správu serverov, ale napríklad aj na ovládanie vetrania alebo klimatizácie v dátovom centre so záznamom teplôt s možnosťou nastavenia hysterézie.

1 Možnosti vzdialeného dohľadu

1.1 Vzdialený dohľad všeobecne

Pojem vzdialeného dohľadu môžeme vysvetliť ako úkon alebo proces, ktorý zabezpečuje starostlivosť a kontrolu nad prevádzkou vzdialených zariadení. Napríklad v sieťových uzloch a to bez nutnosti fyzickej prítomnosti obslužného personálu.

V nie až tak dávnych časoch, boli na takéto úkony určené zodpovedné osoby, ktorých hlavnou pracovnou náplňou bolo zaznamenávanie, kontrola a monitorovanie prevádzky zverených strojov, alebo elektronických zariadení. Získané informácie boli zväčša formou odčítania hodnôt z analógových, alebo segmentových zobrazovacích jednotiek odovzdávané do ústredia, kde boli ďalej spracovávané. Tento proces bol nielen náročný podľa množstva informácií, ale aj dosť zdĺhavý. V prípade poruchy bol najrýchlejším oznamovacím prostriedok telegraf, telefón, alebo kontrolka na monitorovacom paneli.

1.2 Využitie hardvéru pre vzdialený dohľad

Rozmach telekomunikačnej techniky v tomto smere prinieslo obrovské možnosti. Azda najväčším prínosom bola možnosť digitálneho, alebo analógového spracovávania sledovaných hodnôt a zbavenie sa ľudskej chyby. Po zbere digitálnych, alebo analógových hodnôt bolo hneď niekoľko možností, ako dostať tieto informácie v už spracovanom stave na požadované miesto. Za prenosové médium sa volí na základe niekoľkých kritérií. Medzi tieto kritériá patria veci ako: charakter zbieraných informácií, množstvo informácií, možnosti pevnej telekomunikačnej siete, dostupnosť rádiových frekvencií, alebo potreba obojsmerného prenosu. Práve posledná z menovaných podmienok mení celkový pohľad na novodobé dohľadové systémy. Obojsmerný a duplexný prenos sa využíva hlavne v prípadoch, kde je nutný vzdialený zásah po zistení nejakej nezrovnalosti. Takto založené systémy sa využívajú napríklad aj v energetike, kde sa rádiovým ovládajú odpojovače pre vysokovýkonné solárne elektrárne, aby sa zamedzilo poškodeniu distribučnej siete v horúcich letných dňoch. Využívajú sa na to rádiové modemy prevádzkované na licencovaných frekvenciách. Tiež sa často stretávame so základným riešením napríklad cez GSM sieť. Každé riešenie má svoje výhody alebo nevýhody. Rádio modemy prevádzkované na

licencovaných frekvenciách sú výhodné a často z dlhodobého hľadiska aj lacnejšie pre veľké podniky. Dohľadovú sieť majú na tejto technológii vybudované napríklad: Západoslovenská vodárenská spoločnosť, Slovenský plynárenský priemysel, ale aj Dopravný podnik mesta Brno. Jednou z najväčších výhod tejto technológie, je nezávislosť od komerčných telekomunikačných liniek. Na druhej strane, sú tieto frekvencie spoplatňované a ich cenu určuje telekomunikačný úrad na základe parametrov vysielača a počtu účastníckych terminálov. Hlavnými faktormi pri stanovení licenčných poplatkov za frekvencie sú: parametre ako šírka pásma, frekvencia, nadmorská výška antény v kombinácii výšky antény nad terénom a celkový vyžiarovaný výkon. Práve spomínaná šírka pásma je azda najväčším problémom tejto technológie, nakoľko tieto služby sú využívané vo frekvenčných pásmach 160, 300, 400, 900 MHz. V daných pásmach sú vyčlenené úzke kanály o šírke 25 kHz, 12,5 kHz a 6,25 kHz. Prenosová rýchlosť, citlivosť a prístupová metóda môže byť rozličná od výrobcu. Výrobca RACOM pre svoje rádio modemy rady RIPEX udáva prenosové rýchlosti od 11 kb/s pri šírke pásma 6,25 kHz až 83 kb/s pri šírke pásma 25 kHz.



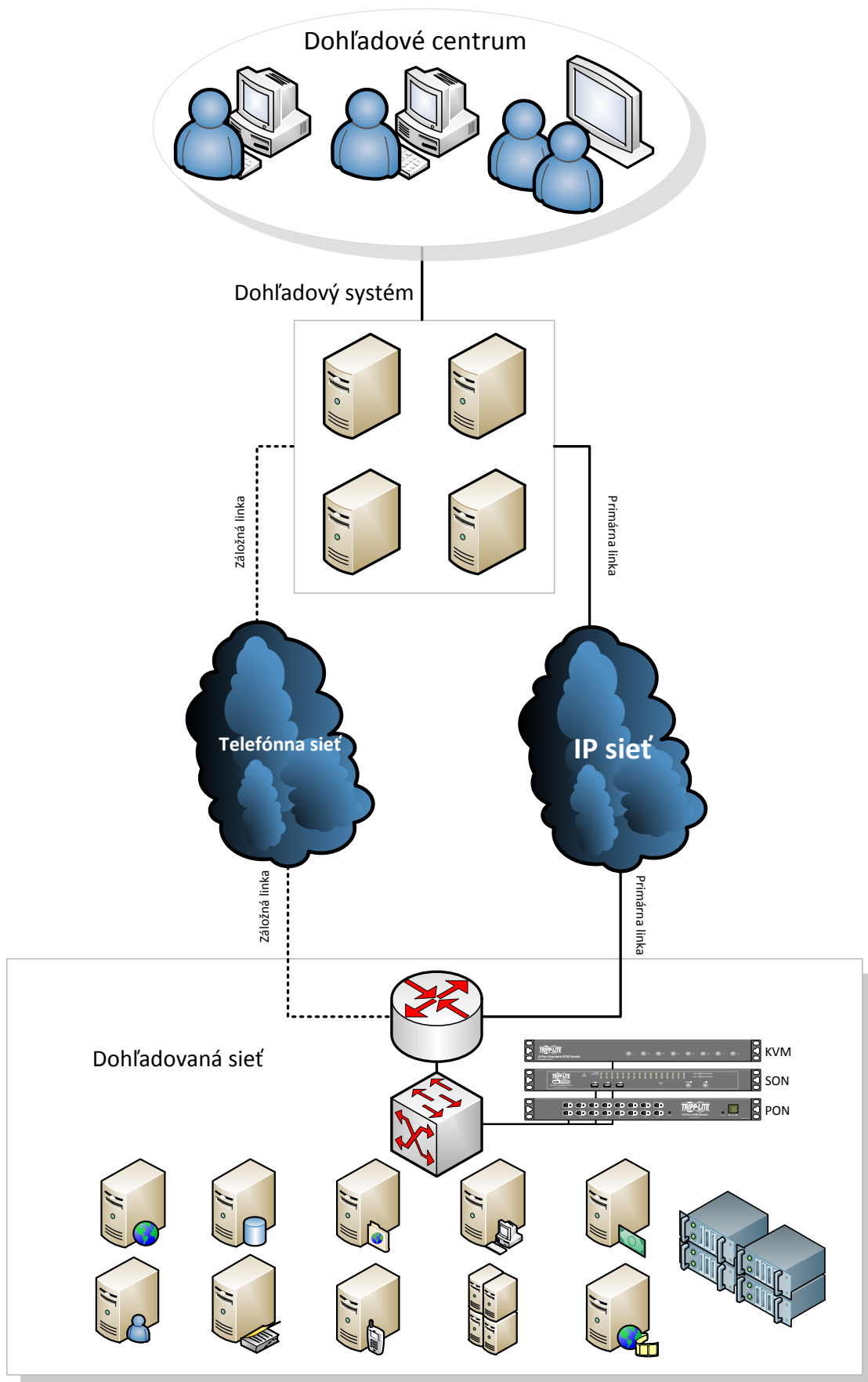
Obr. 1 Rádio modem Ripex s popisom rozhraní

V prípade potreby vyššej prenosovej rýchlosti môžeme siahnuť po GSM / 3G modemoch. Podľa potreby sú dostupné GSM terminály s IP, alebo sériovým výstupom. Mobilné technológie nám umožňujú prenosové rýchlosti od 96 kb/s až po jednotky Mb/s. Celulárna sieť prináša svoje výhody. Hlavnou výhodou je vysoká dostupnosť služieb, avšak prevádzkovanie terminálov je podmienené použitím SIM karty, za ktorú je treba vo väčšine prípadov platiť operátorom na základe množstva prenesených dát! Využívanie akejkoľvek telekomunikačnej siete na samotné prevádzkovanie vzdialeného dohľadu nestačí. Každý výrobca na základe použitej technológie využíva určité komunikačné protokoly zabezpečujúce kanál na monitorovanie a zber požadovaných informácií.

1.3 Využitie softvéru pre vzdialený dohľad

Azda najzaujímavejším miestom pre aplikáciu vzdialeného dohľadu je segment informačných technológií. Pribúdajúci počet zariadení vo firmách, neskôr vo väčších dátových centrách značne komplikovalo ich obsluhu. Technické prostriedky určené na vzdialený dohľad siete sú vo väčšine prípadov univerzálne zariadenia, ktoré do seba integrujú hneď niekoľko užitočných funkcií. Často sa stretávame so škálovateľným riešením, ktoré nám umožňuje kombináciu dohľadového zariadenia s inými prvkami. Podobným spôsobom je možná kombinácia dohľadových zariadení s regulačnou technikou pre účely rôznych odvetví. Rozvoj počítačových sietí akými boli Token Ring, alebo Ethernet, umožnili integráciu služieb dohľadu do existujúcej infraštruktúry. Plnohodnotný obojsmerný prenos dát nám neumožňuje len zber informácií, ale aj zásah do prevádzkovania sieťových prvkov. V rámci sieťovej infraštruktúry sa do operačných systémov najprv začali integrovať prvé protokoly a programové príslušenstvo na kontrolu prevádzky, zberu a analýzy monitorovaných informácií.

Ako jeden z prvých kontrolných protokolov v sieťových operačných systémoch bol ICMP – Internet Control Message Protocol. Tento protokol umožňuje overenie dostupnosti jednotlivých staníc a zariadení v počítačovej sieti jednoduchým príkazom PING. Tento príkaz nám vracia hodnoty dĺžky odozvy v milisekundách a počet skokov cez router označovaného ako TTL – Time To Live. Vzhľadom k tomu, že tento protokol nám poskytuje len základné informácie o stave sieťového zariadenia, pre pokročilejší dohľad sa najčastejšie využíva protokol SNMP – Simple Network Management Protocol.



Obr.: 2 Schéma vzdialeného dohľadu telekomunikačnej siete so zálohou

Protokol SNMP nám umožňuje vyčítavanie hodnôt z MIB tabuľky. MIB tabuľku nám poskytuje výrobca a obsahuje štruktúru vyčítateľných hodnôt akými sú napríklad: vyťaženie procesora, využitie pamäte, napätie na zdroji alebo prevádzka na sieťovom rozhraní. Týmto protokolom získané informácie môžu slúžiť na generovanie grafov, alebo alarmov. Túto časť práce už vykonávajú softvérom riadené dohľadové systémy, ktoré môžu byť použité v podstate na čokoľvek. Samotný koncept monitorovania na báze klient – server v IP sieti bol štandardizovaný pod názvom RMON – Remote Monitoring MIB. Monitorovanie štandardom RMON v sebe zahŕňa 9 parametrov pre monitorovanie IP sietí, ktoré sú popísané v tabuľke č. 1. Prvá definícia tohto štandardu bola iba pre protokol Ethernet (RFC 1271) a neskôr sa špecifikácia rozšírila aj na Token Ring (RFC 1513). Dané štandardy do seba ďalej integrujú protokoly ako NetFlow, alebo SFlow, ktoré slúžia na zber informácií o sieťovej prevádzke. Tieto protokoly zaznamenávajú informácie z hlavičiek paketov. Z toho vieme určiť veľkosť paketu, zdrojovú, cieľovú IP adresu a komunikačný port.

Tab. 1: Popis parametrov jednotlivých skupín štandardu RMON

	SKUPINA	POPIS
1	Statistics	Zber údajov zo siete. Obsahuje informácie globálneho charakteru ako celkový počet kolízií, celkové zaťaženie siete a podobne.
2	History	História globálnych záznamov, z ktorých sa generujú štatistiky.
3	Alarms	Nastavenie prahových hodnôt - thresholdov, po ktorých sa uskutoční vopred definovaná akcia.
4	Hosts Table	Záznam prevádzky aktívnych zariadení v sieti na základe IP alebo MAC adresy. Berú sa do ohľadu parametre ako počet prijatých a odoslaných paketov.
5	Hosts Top N	Záznam prevádzky najaktívnejších zariadení v sieti v špecifikovanej časovej perióde.
6	Matrix	Štatistika prenosu dát medzi jednotlivými zariadeniami v sieti.
7	Events	Udalosti, ktoré sú zaznamenávané po prekročení vopred definovaných prahových hodnôt. Môžeme ďalej špecifikovať úkon, ktorý sa má vykonať. Napríklad odoslanie alarmu do mailu alebo SMS.
8	Filters	Nastavenie podmienok pre generovanie štatistík. Napríklad zdrojová / cieľová IP adresa, alebo špecifikácia komunikačného portu.
9	Packet Capture	Odchytávanie paketov a ich preposielanie nejakému diagnostickému nástroju. Umožňuje podrobnú real time analýzu sieťovej prevádzky.

1.4 Dohľadové systémy a dohľadové centrá

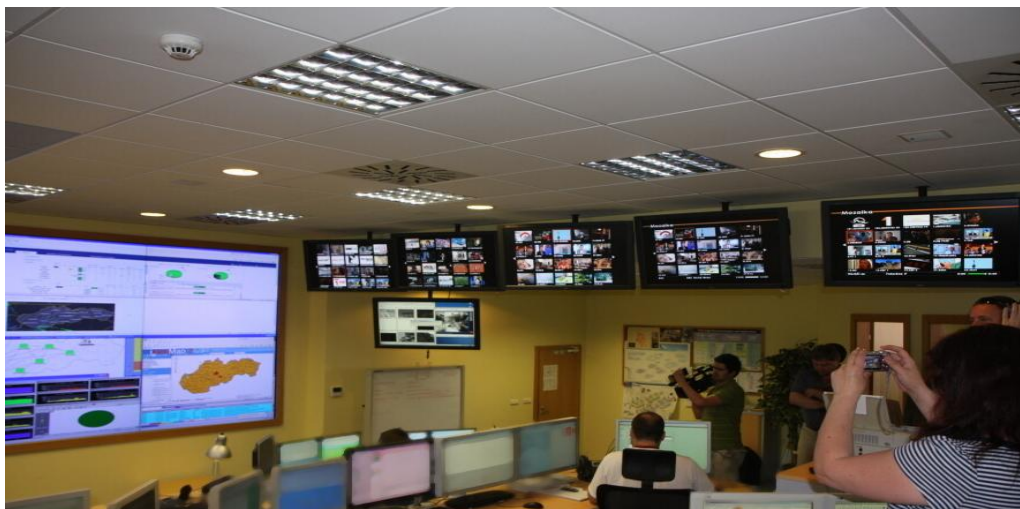
Softvérové dohľadové systémy sa využívajú na podrobnejšie spracovanie získaných informácií zo zariadení. Vďaka nim sme schopní rýchlo reagovať na akékoľvek problémy reportované týmto systémom. Môžu byť nastavené prahové hodnoty určujúce nebezpečný stav, po ktorom je nutný zásah. Takéto systémy sú vo veľkom využívané telekomunikačnými operátormi. Poskytuje im to veľmi presný prehľad o aktuálnom stave siete. Od dohľadu nad elektrinou, teplotou v rozvádzačoch alebo dostupnosti telekomunikačných zariadení až po sledovanie preťaženia sieťových uzlov. Záleží to len na schopnostiach samotného softvéru.

Najrozšírenejšie dohľadové Open Source systémy využívané menšími organizáciami sú Nagios, Cacti, alebo MRTG, ktorých kombinácie využíva väčšina malých a stredných internetových operátorov. Okrem toho, že sa jedná o bezplatný systém, je schopný kontrolovať nielen dostupnosť zariadení v sieti, ale aj služby bežiacie na zariadeniach. Napríklad dostupnosť webovej služby na webovom serveri. Užitočnou vlastnosťou tohto systému je aj možnosť kombinácie s SMS bránou, ktorý umožňuje zasielanie SMS správ technikom v prípade poruchy. Podobné riešenie nám prináša aj dohľadový softvér DUDE od Mikrotiku. Na rozdiel od Nagiosu sa jedná o robustnejšie, ale žiaľ o menej spoľahlivé riešenie. DUDE nám umožňuje grafovanie prevádzky na sieťových rozhraniach s možnosťami nastavenia prahových hodnôt. Sledované sieťové zariadenia môžeme premietnuť do mapy, čo nám sprehládni celkový dohľad nad sieťou.

Väčšina veľkých internetových, alebo mobilných operátorov využíva špeciálny dohľadový systém, ktorý je priamo integrovaný do ich informačného systému. Medzi takéto systémy patria aj systémy ako HP OpenView, alebo IBM Tivoli. Obe riešenia v sebe zahŕňajú škálovateľnosť pre sieťový dohľad o organizáciu IT infraštruktúry. Tieto špičkové komerčné systémy sú kombinovateľné s modulmi tretích strán a tým pádom nie sú viazané na zariadenia výrobcu dohľadového systému. Výstupné údaje sú zocelené a spracovávané v jednom, spoločnom prostredí. Takéto riešenie umožňuje správu veľkého množstva vzdialených zariadení. Tým, že sú tieto dohľadové systémy priamo integrovateľné do informačných systémov, je možné vytvoriť akúsi spätnú väzbu a z časti automatizovať chod telekomunikačných zariadení v sieti. Takéto funkcie sú využívané aj v kombinácii s Power Over the NET. V prípade nedostupnosti sieťového uzlu, väčšinou odľahlej vysielacej stanice, dohľadový systém pošle príkaz na

zariadenie Power Over the NET a ten vykoná krátky reštart jedného zo zvolených zariadení v rozvádzači. Prostredníctvom protokolu SNMP je možné získavať dáta z väčšiny zariadení rady Over the NET.

Okrem dohľadu nad sieťovými prvkami, na ktoré postačuje KMV, Power Over the NET, Serial Over the NET sa kladie čoraz väčší dôraz na dohľad IPTV ústrední. Najpoužívanejšou formou dohľadu nad IPTV Headendom je softvérová kontrola a analýza bežiacich multicastových skupín. V rámci tejto metódy sa používa spôsob sledovania prenosovej rýchlosti jednotlivých staníc. Táto metóda žiaľ neošetrí náročnejšie problémy napríklad s kódovaním, alebo dekódovaním jednotlivých staníc. Pre tieto účely sú určené špeciálne dohľadové systémy, ako napríklad CISCO ROSA, ktorý plne spolupracuje s výrobkami spoločnosti CISCO a SCIENTIFIC Atlanta. Tieto špeciálne dohľadové systémy majú okrem protokolu SNMP aj špeciálny komunikačný protokol, ktorým je IIOP. Protokol IIOP zabezpečuje obojsmernú komunikáciu na vyčítavanie aj zápis nastavení do autorizovaných zariadení v dohľadovom systéme. Systém CISCO ROSA ponúka širokú škálu možností, z ktorých je väčšina licencovaná a užívateľ si jednotlivé funkcie systému musí zvlášť zakúpiť. Toto prevedenie je dostupné v softvérovom, ale aj plne hardvérovom prevedení. Žiaľ, jedná sa o podstatne drahšie riešenie ako je to v prípade KMV, Power Over the NET, Serial Over the NET. Služby digitálnej televízie sú náročnejšie na reakčný čas v prípade vyskytnutia nejakých problémov. Veľmi jednoduchou, a tiež často používanou metódou je mozaika. Tento spôsob dohľadu využíva aj spoločnosť Orange pre kontrolu nad službami Fiber TV, ako je to možné vidieť aj na obrázku č.: 3.



Obr. 3 Dohľadové centrum spoločnosti Orange Slovensko a.s.

2 KVM Over the NET

KVM, v skratke klávesnica, video, myš je označenie zariadení, ktoré slúžia na pohodlnejšie ovládanie viacerých zariadení z jedného miesta. Z počiatku sme poznali len pasívne KVM zariadenia, ktoré boli inštalované v rozvádzačoch a boli pripojené na lokálny monitor, myš a klávesnicu. Za pomoci mechanického prepínača sme si mohli zvoliť zariadenie, ktoré chceme ovládať. Neskôr pribudli aktívne KVM prepínače, ku ktorým sme si mohli pripojiť zdieľané zariadenia aj prostredníctvom USB. Pri niektorých aktívnych KVM prepínačoch sú zabudované funkcie prepínania za pomoci klávesových skratiek. Výhodou aktívnych KVM v takýchto prípadoch bolo pohodlné a rýchle použitie jedného monitora, klávesnice a jednej myšky na ovládanie niekoľkých zariadení v rozvádzači, avšak nie súčasne. Prevrat medzi týmito zariadeniami priniesli až takzvané IP KVM zariadenia, ktoré umožnili správcovi siete nielen vzdialený prístup, ale aj prácu na súčasne viacerých zariadeniach naraz. IP KVM označované aj ako KVM over IP umožnili pohodlnejšiu správu zariadení, bez ohľadu na vzdialenosť umiestnených serverov a to ako cez internet tak aj cez lokálnu sieť. Správca si na týchto zariadeniach môže vytvoriť oddelené užívateľské účty. Jednotlivých užívateľov na viacvýstupovom KVM over IP vieme priradiť ku konkrétnym výstupom na KVM prepínači a tým pádom vieme poskytnúť bezpečný vzdialený manažment serverov aj iným, navzájom oddeleným užívateľom. Osobne považujem použitie technológie KVM v dátových centrách, alebo pri vzdialenom prevádzkovaní serverov za nevyhnutnosť, nakoľko vzdialená plocha nám neumožní 100 percentnú ovládateľnosť počítača. V opačnom prípade sa často stane, že správca siete musí precestovať desiatky, ba až stovky kilometrov za účelom oživenia serveru, alebo obyčajnému prestaveniu parametrov napríklad v BIOSe. Dokonca po niekoľkých zlých skúsenostiach prevádzkovania serverov v asi 110 kilometrov vzdialenom peeringovom centre, ktoré je v našom hlavnom meste, Bratislave, som sa žiaľ aj ja osobne poučil a používanie zariadenia KVM over IP už považujem ako základ pri podobných aplikáciách. Ako zlatú kombináciu považujem použitie zariadení KVM, Serial over IP a Power over NET. Zaujímavou záležitosťou KVM prepínačov je nezávislosť od operačného systému zariadenia, ktoré chcem ovládať. KVM prepínač sa tvári ako keby na počítače boli priamo pripojené vstupno-výstupné zariadenia. Väčšina aktívnych KVM prepínačov majú funkciu HOTPLUG, ktorá umožňuje pripojenie alebo odpojenie počítača aj vtedy,

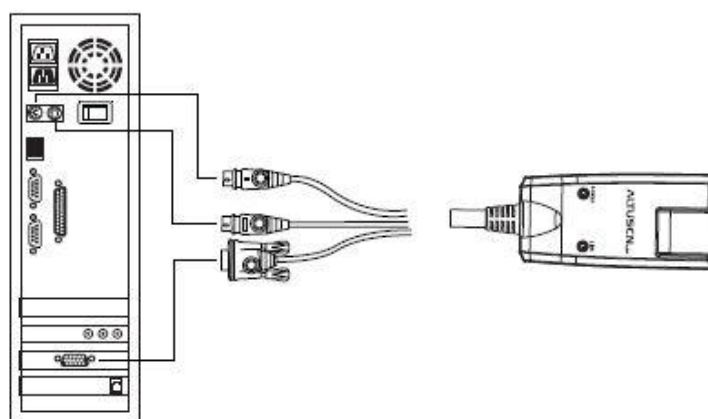
keď už počítač beží. Za poznamenanie stojí kombinácia KVM prepínača s monitorom, klávesnicou a myškou v 19 palcovom prevedení, ktoré je určené pre dátové rozvádzače. Jedná sa o aktívny KVM prepínač, ktorý je navrhnutý hlavne za účelom úspory miesta v rozvádzačoch, nakoľko si často nemôžeme dovoliť obsadiť drahé miesto v prenajatom dátovom rozvádzači klasickým monitorom.

KVM prepínače nám dnes už ponúka niekoľko, nielen renomovaných výrobcov. Jednotlivé zariadenia sa líšia len minimálne. Hlavný dôraz pri zaobstarávaní kladíme na spoľahlivosť a samozrejme na cenu. Ceny sa medzi výrobcami veľmi nelíšia. Drastický rozdiel nastáva, keď si porovnáme ceny bežných aktívnych KVM prepínačov, alebo KVM over IP prepínačov. Na porovnanie sú KVM over IP prepínače asi za trojnásobok ceny v porovnaní s bežnými aktívnymi KVM prepínačmi. Cenu nám stanovuje hlavne počet portov, čiže počet pripojiteľných zariadení, ktoré chceme prostredníctvom KVM prepínača ovládať. Pri kúpe si musíme uvedomiť, koľko zariadení chceme ovládať, akým spôsobom a hlavne, že kde sa majú KVM prepínače inštalovať. Pre prípad dátového rozvádzača, by som volil 19 palcové 16 portové prevedenie, samozrejme s prístupom cez IP. Pre menšie aplikácie, sú dostupné takzvané SOHO riešenia, ktoré sa dajú zakúpiť aj v konfigurácii s dvoma až dvanástimi výstupmi. Pri týchto prepínačoch je zväčša možné prepínanie medzi zariadeniami za pomoci klávesovej skratky, alebo za pomoci inštalovaného softvéru dodaného výrobcom zariadenia. Štandardnými rozhraniami na pripojenie počítačov sú monitorový port VGA alebo SVGA, PS/2 pre myš aj klávesnicu, prípadne USB.

V práci sa naďalej budeme zaoberať KVM over IP prepínačom KH-1516i od spoločnosti ATEN. Jedná sa o prepínač, ktorý je v 19 palcovom prevedení o výšky 1U určená pre dátové rozvádzače. Sú to veľmi kvalitné zariadenia, ktoré používa veľká väčšina operátorov. Avšak toto zariadenie nie je jediné z ponuky deklarovaného výrobcu. Najmenší model viac portového KVM over IP je zariadenie s označením CS1708i. Umožňuje pripojenie 8 zariadení na PS/2 a USB. Tento KVM prepínač môže ovládať 32 súčasne pripojených užívateľov. Pre najnáročnejších užívateľov je určený model s označením KN4132, ktorý umožňuje pripojenie až 32 zariadení. Každé je ovládateľné na úrovni BIOSu, čo znamená že tento KVM prepínač v plnom rozsahu nahradzuje lokálne pripojený monitor, klávesnicu a myš. Pripojené zariadenia môže ovládať až 32 pripojených užívateľov na najvyššej úrovni. K pripojeniu zariadení ku

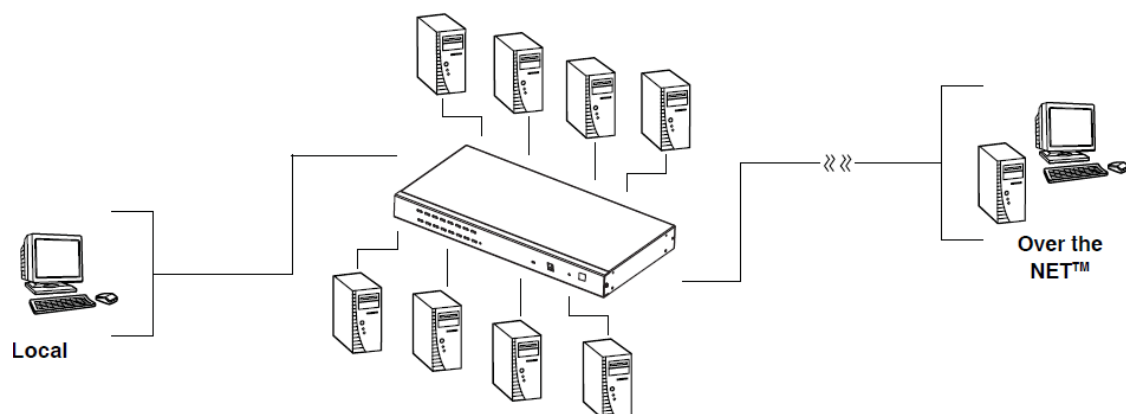
KVM prepínaču je nutné použiť moduly dodávané výrobcom. Rozširovacie moduly sú rovnaké ako v prípade nami testovaného KVM prepínača KH-1516i.

Zariadenie ATEN KH-1516i má 16 portov, čiže sme schopní pripojiť až 16 zariadení. Ku každému zariadeniu je nutné pripojiť rozbočovací KVM modul, nakoľko na zariadení máme len rozhranie na konektor RJ45. Je to z dôvodu možnosti použitia dlhších káblov ku koncovým zariadeniam a úspory miesta. Vďaka tomuto môžeme ovládať zariadenia aj v iných, vzdialenejších rozvádzačoch. Avšak narastajúcou dĺžkou kábla narastá aj odozva na nami vykonané operácie. Výrobca udáva maximálnu dĺžku sieťového kábla kategórie 5e 30 metrov pre rozlíšenie 1600 x 1200 pri frekvencii 60 Hz. 40 metrov môžeme dosiahnuť pri nižšom rozlíšení a to pri 1280x1024 a frekvencii 75 Hz. Jednou z ďalších výhod tohto zariadenia je, že ho môžeme využiť aj ako lokálny KVM prepínač. Pripojené zariadenie môžeme ovládať cez IP protokol ale aj cez lokálny monitor, klávesnicu a myš zároveň. Zariadenie, ktoré chceme ovládať lokálne, môžeme vybrať priamo na prednom paneli KVM prepínača. Ako sme vyššie spomínali, na pripojenie počítača ku KVM prepínaču je nutný KVM modul. Výrobca dodáva niekoľko KVM modulov s rôznymi označeniami, ktoré sa pripájajú na rôzne rozhrania stanice. Za pomoci modulu KA9520 pripojíme klávesnicu PS/2, myšku PS/2 a monitor VGA alebo SVGA. Modul KA9170 nám zasa umožňuje pripojenie monitora VGA alebo SVGA a USB, modul KA9570 umožňuje pripojenie dátovej siete a monitora a modul KA9130 nám umožní pripojenie klávesnice PS/2 a monitora VGA alebo SVGA.



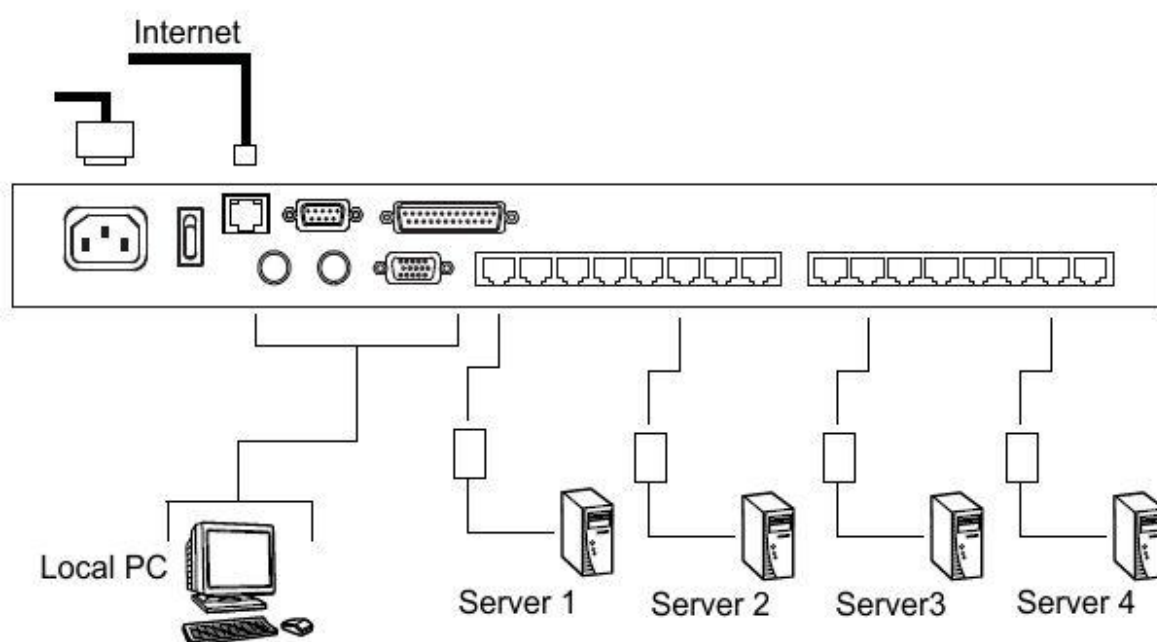
Obr. 4: Modul KA9520 určený pre KVM prepínač ATEN KH-1516i

Každý z modulov je možné kedykoľvek za chodu pripojiť, alebo odpojiť od KVM prepínača, alebo od stanice. Na koniec tejto hrubej špecifikácie by som rád spomenul spotrebu zariadenia pre prípadnú zálohu, v prípade výpadku elektrickej energie, ktorá sa pohybuje na úrovni 12W, pričom je táto hodnota pre nás viac než priaznivá!



Obr. 5: Schéma celkového zapojenia KVM prepínača ATEN KH-1516i

Základnú konfiguráciu zariadenia ATEN KH-1516i a jednotlivých portov môžeme vykonať aj za pomoci priamo pripojeného monitora, klávesnice a myšky.



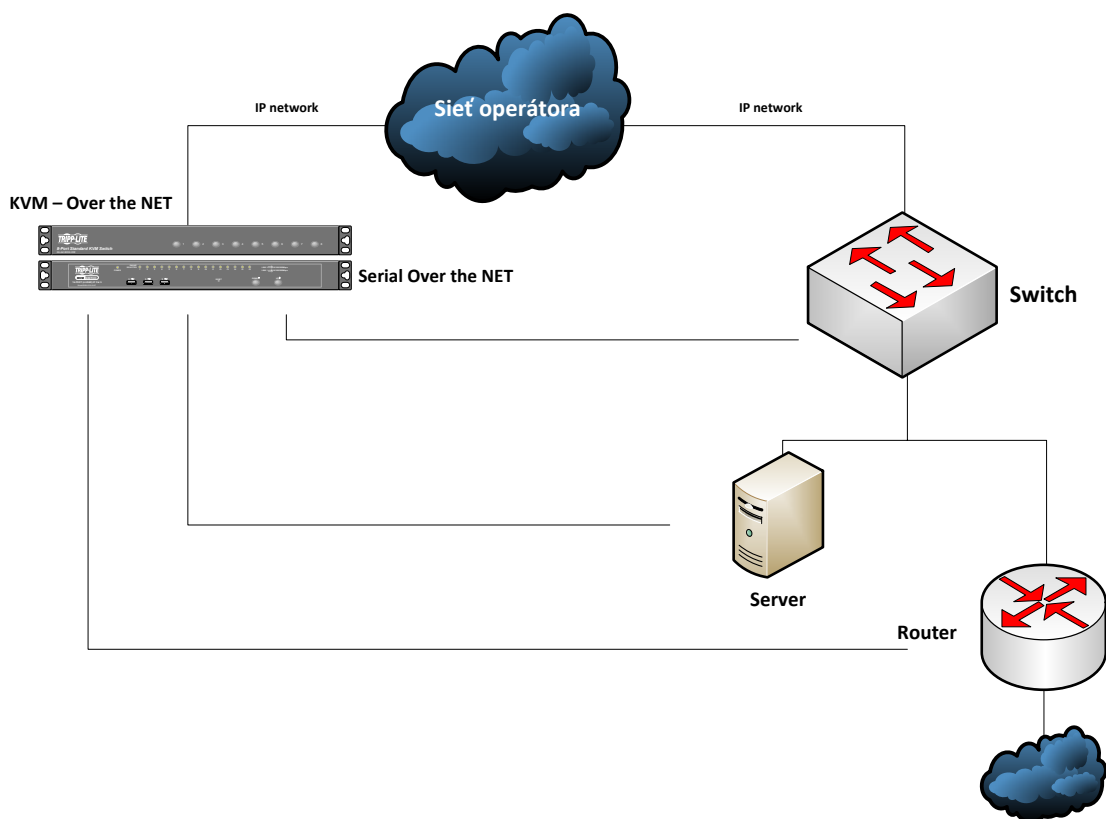
Obr. 6: Zadný panel KVM prepínača ATEN KH-1516i

Pre podrobnejšie a pohodlnejšie nastavenia sa budeme musieť prihlásiť cez IP adresu prostredníctvom webového prehliadača. Štandardná IP adresa je 192.168.0.60. Prihlasovacie meno je administrator a heslo password. V prípade nedostupnosti zariadenia pod touto IP adresou, treba skúsiť pripojiť špecifický port na DHCP server, nakoľko funkcia DHCP klienta je v základnom nastavení zapnutá. Po prihlásení sa, je nastavenie veľmi jednoduché a prehľadné. Zariadenie ATEN KH-1516i má plne prepracované webové rozhranie, prostredníctvom ktorého vieme nastaviť všetky nami požadované nastavenia. Prihlásiť sa je možné ako cez http protokol, tak aj cez šifrovaný https protokol, ktorý nám poskytne maximálnu úroveň bezpečnosti.

Po prihlásení sa, povereniami správcu dostaneme prístup ku všetkým meniteľným parametrom zariadenia. Z tohto dôvodu rozdeľujeme užívateľov na 2 skupiny. Administrátor, užívateľ s povereniami správcu a bežných užívateľov, ktorí majú prístup len ku správcom definovaným portom na KVM prepínači. Priamo cez úvodnú obrazovku po prihlásení vidíme všeobecné informácie o našom KVM prepínači, ktoré nám umožní ľahšiu identifikáciu zariadenia v sieti. Tieto informácie sú nápomocné hlavne pri väčšom množstve KVM prepínačov v sieti. V bodoch menu, na ľavej lište webového rozhrania si môžeme vybrať z niekoľkých spôsobov pristupovania ku pripojeným zariadeniam. V prípade, že na klientskom počítači používame operačný systém Windows, máme k dispozícii klienta na stiahnutie priamo cez web rozhranie KVM prepínača. V opačnom prípade máme možnosť použiť univerzálny spôsob pristupovania, cez JAVA aplikáciu, ktorú nám vygeneruje KVM prepínač podľa aktuálnych nastavení. V prípade, že máme k dispozícii len bežné užívateľské oprávnenie, tak po prihlásení vidíme možnosť pripojenia len na konkrétny, správcom konfigurovaný port. Táto voľba je veľmi rozšírená pre zákazníkov serverhousingu v dátových centrách niektorého z operátorov. Takýto spôsob pristupovania umožní zákazníkovi pohodlný prístup a spôsob pripojenia sa na svoj server na najvyššej úrovni. Nami testovaný KVM prepínač ATEN KH-1516i umožňuje aj autorizáciu užívateľov prostredníctvom RADIUS serveru, čím zjednoduší celkovú správu užívateľov! V prípade akýchkoľvek problémov je možné zariadenie ATEN KH-1516i vrátiť do výrobných nastavení. Jedným zo spôsobov je vykonať reset zariadenia cez webové rozhranie. V prípade, že IP adresu KVM prepínača nevieme, prepínač môžeme resetnúť cez mikro tlačítko na prednom paneli.

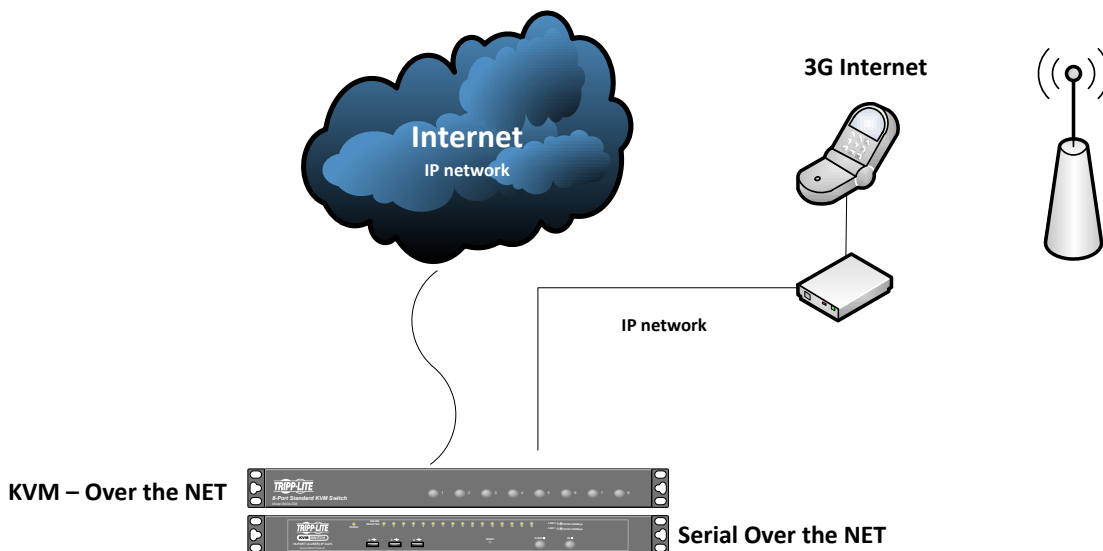
O dôležitosti KVM prepínačov vedia svoje systémoví inžinieri, ktorí aplikujú vzdialené aktualizácie, ktoré si vyžadujú zásah so samotného jadra operačného systému. Takéto aktualizácie si ešte nedávno vyžadovali fyzickú účasť technika pri servery, čo bolo nielen časovo, ale aj finančne náročnejšie hlavne pre klienta.

V prípade inštalácie akéhokoľvek zariadenia slúžiaceho na dohľad nad uzlami telekomunikačnej siete musíme dbať na jeho správne osadenie, integráciu do stávajúceho systému. V každom prípade by malo byť dodržané určité hierarchické vrstvenie a vetvenie, ktoré by nám malo zabezpečiť funkcionality monitorovacieho zariadenia aj v prípade akéhokoľvek výpadku dohliadaného zariadenia. V jednoduchosti to znamená, že internetovú alebo intranetovú konektivitu na KVM prepínač, Power Over the NET, alebo Serial Over the NET nebude zabezpečovať ten prepínač, router alebo iné zariadenie, ktorého funkčnosť máme prostredníctvom týchto monitorovacích prvkov zabezpečiť.



Obr. 7: Schéma ideálneho zapojenia KVM prepínača a zariadenia Serial Over the NET

V ideálnom prípade by na tieto zariadenia mohla byť pripojená konektivita z nezávislej siete, ktorej funkčnosť nebude monitorovacími prvkami ovplyvnená. Pre pokročilejšie aplikácie môžeme využiť internetovú konektivitu od iného, nezávislého operátora, alebo aj 3G modem. V prípade, že to umožňuje samotné monitorovacie zariadenie, vieme použiť obe pripojenia súčasne, a tým zabezpečíme ešte väčšiu flexibilitu a efektivitu v prípade riešenia krízovej situácie. Základnou požiadavkou je mať zariadenú verejnú IP adresu a ak je to možné tak statickú. V prípade, že sú dohľadové zariadenia za smerovačom, za ktorým nemáme rozsah verejných IP adries, je nutné vykonať presmerovanie portov. Pre služby telnetu je nutné presmerovať port TCP 23 zo strany verejnej IP adresy na lokálnu adresu zariadenia. V prípade väčšieho počtu zariadení môžeme zdrojové porty zmeniť, avšak cieľový musí ostať štandardne prislúchajúci danej službe.

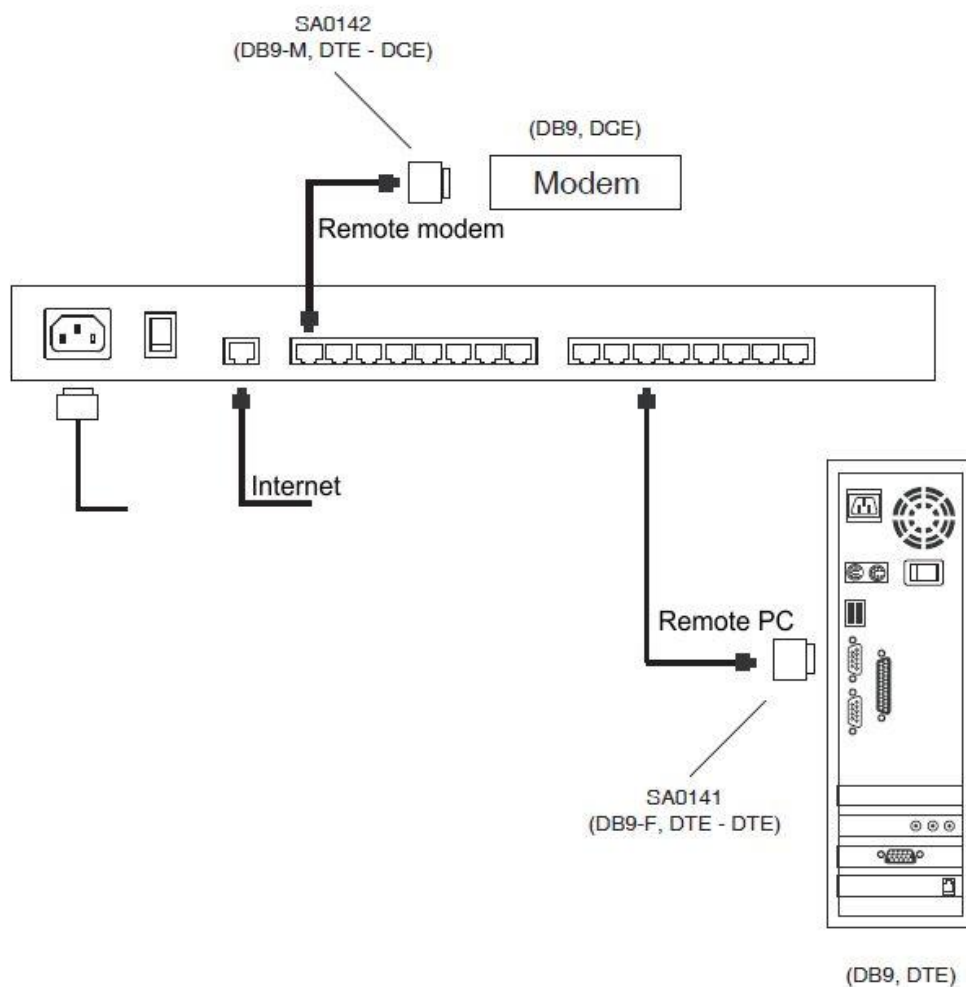


Obr. 8: Znázornenie redundantného pripojenia Internetu k prvkom dohľadu

3 Serial Over the NET

Zariadenie ATEN SN-0116 slúžia na vzdialené pripojenie sériového komunikačného rozhrania zariadenia prostredníctvom IP protokolu. Sú plnohodnotnou náhradou priamo pripojeného sériového kábla. Pri spomínanom zariadení máme v podstate neobmedzené možnosti vzdialeného manažmentu zariadení ako sú prepínače, routre, servery a iné sieťové zariadenia. Vo väčšine prípadov nám sériové rozhranie umožní ovládať zariadenie, aj keď správca siete z nejakého dôvodu pokazí konfiguráciu napríklad cez SSH. Zväčša sa stáva, že sa nedopatrením preruší spojenie na spravovanom zariadení. Pomocou IP protokolu je z dôvodu zlej konfigurácie manažment nedostupný a jedna z možností, ako túto chybu napraviť je reštart zariadenia, ktorý je nápomocný len v prípade, že zlé nastavenia sa neuložili. Rýchlejšim spôsobom je úprava konfigurácie zariadenia prostredníctvom komunikačného rozhrania. Na riešenie tejto problematiky sú vyrábané zariadenia z rady Serial over NET od spoločnosti ATEN.

Zariadenia z rady Serial over NET od spoločnosti ATEN sú vyvinuté a v drvivej väčšine prípadov aj aplikované na vzdialenú správu telekomunikačných zariadení a serverov v dátových centrách telekomunikačných operátorov. Umožňujú vzdialený prístup na viaceré sériové rozhrania. Výrobca Aten nám ponúka niekoľko zariadení z rady Serial over NET. Pre najjednoduchšie aplikácie môžeme použiť model SN3101, ktorý nám umožní pripojiť len jedno zariadenie prostredníctvom sériového rozhrania. Na takéto jednoduchšie aplikácie operátori s obľubou využívajú zariadenia Mikrotik Routerboard, ktoré je možné tiež nakonfigurovať popri inom ako aj Serial over IP. Pre náročnejšie aplikácie sú určené zariadenia od Atenu SN-0108 s možnosťou pripojenia 8 zariadení alebo SN-0116 s možnosťou pripojenia až 16 zariadení. Prístup na samotné zariadenie ATEN SN-0116 je možný cez protokol telnet, ssh, alebo aj cez web rozhranie.



Obr. 9: Zadný panel zariadenia ATEN SN-0116 s ilustráciou prepojiteľnosti

Po prihlasovaní sa cez telnet, alebo ssh užívateľ vidí hlavné menu, cez ktoré sa po overení užívateľských práv dopracuje k možnosti výberu spravovania konkrétneho zariadenia, pričom prístupy a oprávnenia k jednotlivým zariadeniam musia byť vopred nastavené správcom. Pri konfigurácii je vopred nutné nastaviť prenosovú rýchlosť sériového rozhrania, počet bitov, paritu, stop bity a spôsob riadenia toku, ktoré sú zväčša udané výrobcom pripájaného zariadenia. V praxi sa tieto rýchlosti pohybujú v rozmedzí 1200 až 115200 baudov pre rozhranie RS-232. Pre rýchlejší prístup prostredníctvom telnetu, alebo ssh môžeme danému komunikačnému rozhraniu prideliť port, na úrovni IP protokolu, prostredníctvom ktorého budeme môcť priamo pristupovať na zvolené zariadenie. Ako aj v prípade ostatných zariadení od spoločnosti ATEN, máme širokú možnosť riadenia užívateľských účtov. Správa zariadenia môže vytvoriť samostatné, navzájom oddelené užívateľské účty, prostredníctvom čoho budú môcť

jednotliví užívatelia bezpečne manažovať svoje zariadenia. Pre pohodlnejšie ovládanie výrobca bezplatne dodáva software, pomocou ktorého môžeme do nášho počítača nainštalovať a namapovať virtuálne sériové rozhranie pre vzdialené komunikačné rozhranie, ktoré bude samozrejme pracovať cez IP protokol. Za pomoci tejto aplikácie sa namapuje fyzické rozhranie na zariadení ATEN na virtuálne rozhranie v našom počítači. Toto riešenie nám umožní oveľa väčšiu efektivitu a dynamiku využívania tohto zariadenia. Táto funkcia nám taktiež umožní plnohodnotné prepojenie na sériové rozhranie modemu. Aplikácia sa nazýva Real COM port management a je aj voľne dostupná na stránkach výrobcu. Inštalácia je podporovaná na operačných systémoch Windows aj Linux.

Jednotlivé zariadenia sa pripájajú prepojovacími káblami, ktorých jedna strana je zakončená bežným konektorom typu RJ45 a druhá strana je zakončená požadovaným rozhraním podľa typu sériového rozhrania. Zväčša DB9 alebo DB 25.



Obr. 10: Zapojenie konektora RJ45-F - DB9-F

Maximálna dĺžka kábla je závislá od konkrétneho rozhrania. Pre rozhranie RS-232 je to približne 15 metrov. Tieto mnou deklarované prepojovacie káble výrobca štandardne v balení so zariadením nedodáva. Z tohto dôvodu sme pri pokusoch používali štandardné konfiguračné Cisco káble pre sériové rozhranie typu RJ45-F - DB9-F.

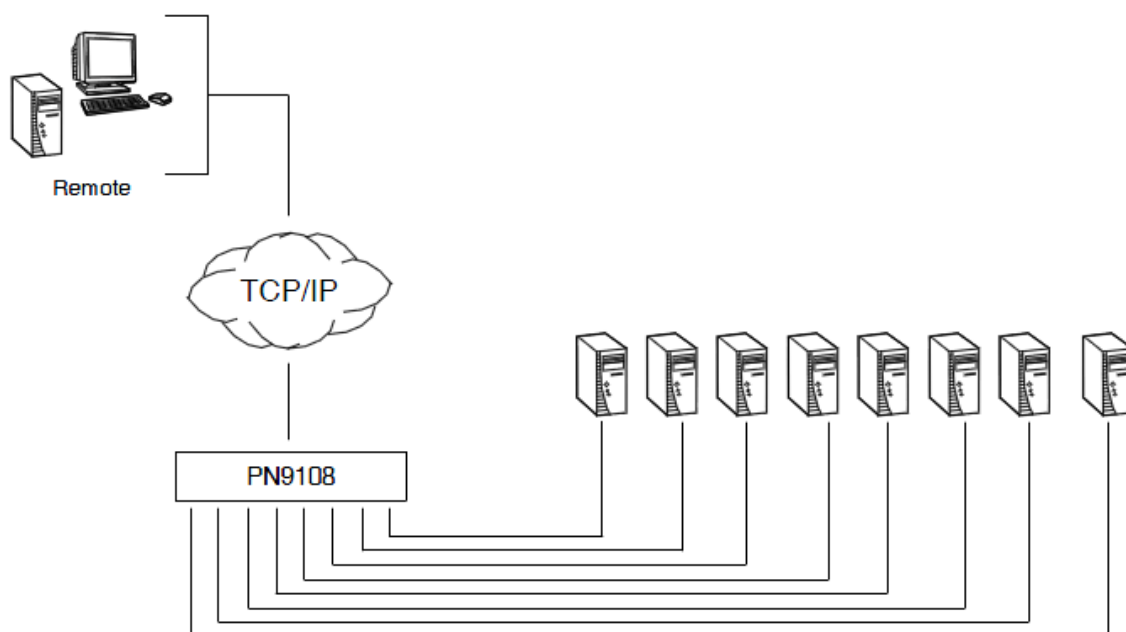
Na trhu je dostupná celá rada podobných zariadení, ktoré sa líšia hlavne prevedením a počtom pripojiteľných zariadení. Jednoduchšie z nich nie sú konštruované na inštaláciu v dátových rozvádzačoch a majú menej rozhraní na pripojenie jednotlivých

zariadení. Tieto zariadenia nachádzajú uplatnenie hlavne ako konvertory pre zberače dát, ktoré sú veľmi rozšírené v teplárskom a vodárskom priemysle. Na základe požiadaviek daných odvetví už dnes existuje niekoľko nadstavieb týchto zariadení, ktoré sú zväčša rozšírené o rádiový modem alebo GSM/GPRS jednotku. Jedným z dodávateľov podobnej technológie je aj česká spoločnosť Racom. Tiež je dostupná celá škála možností vyrobiť si vlastné zariadenie Serial Over the NET z vlastného počítača. Stačí správne programové vybavenie vzhľadom na operačný systém. Niekoľko programov je dokonca bezplatných a umožňujú nie len pripojenie zariadenia cez sériový port, ale aj prenos dát cez sériové rozhranie v kombinácii s IP sieťou. Výhoda tohto prevedenia je, že sme schopní prenášať hodnotu napäťovej úrovne cez IP sieť. Táto vlastnosť nám umožňuje aj prevádzkovanie takzvaného vzdialeného paketového rádia napríklad cez CB. Podmienkou na prevádzkovanie takéhoto prenosu je možnosť zvoliť si na prenos virtuálne sériové rozhranie.

Pre pokročilejší zber telemetrických údajov bola nedávno uvedená na trh novinka od spoločnosti ATEN pod označením Guardian Over the NET - GN0116. Jedná sa o zariadenie, ktoré je osadené väčším množstvom vstupných aj výstupných rozhraní. Toto konkrétne zariadenie má 4 analógové vstupné porty odporového typu, 2 analógové vstupné porty napäťového typu, 2 digitálne vstupné porty a 8 digitálnych výstupných portov. Každý z týchto portov je individuálne kontrolovateľný a môže slúžiť aj na ovládanie menšieho dátového centra, alebo iných priestorov počnúc od detekovania otvorených dverí po dymové senzory, vzduchotechniku, núdzové osvetlenie a vzhľadom k rôznorodosti vstupných a výstupných rozhraní k mnohým iným riešeniam. Veľkou výhodou tohto zariadenia, ako je tomu v prípade väčšiny zariadení od Atenu, je ich škálovateľnosť. V tomto prípade vieme pripojiť do reťazca až 255 jednotiek.

4 Power Over the NET

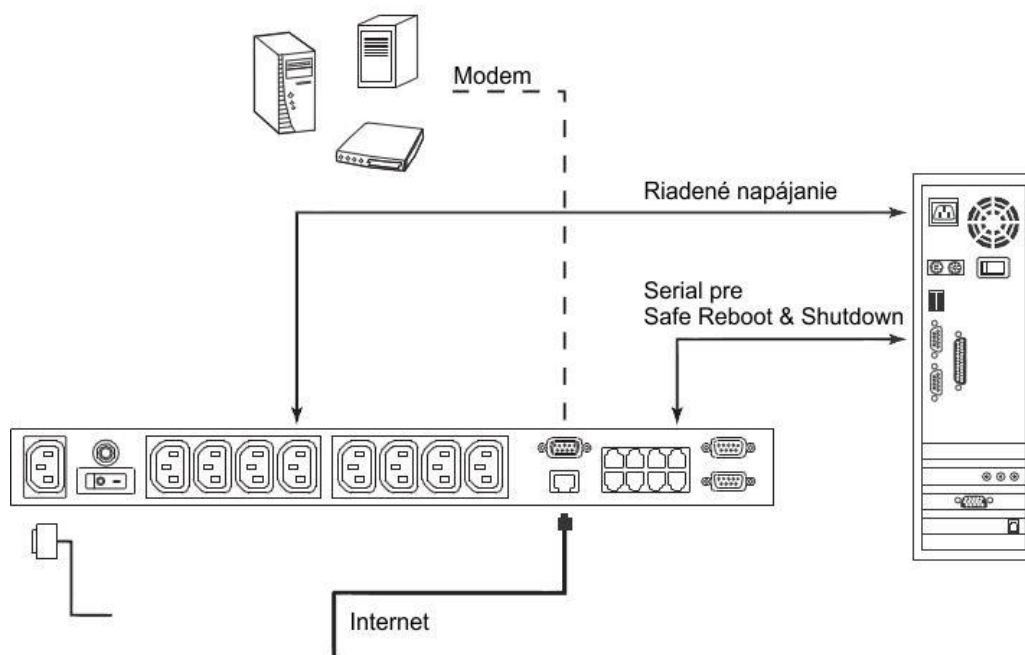
Posledným zariadením zo zadania je ATEN PN-9108. ATEN PN-9108 je určený na vzdialenú správu napájania elektronických spotrebičov. V našom prípade sa jedná o pracovné stanice, servery, smerovače a prepínače. Zariadenie ATEN PN-9108 je v 19 palcovom prevedení, čiže je určené na inštaláciu v dátových rozvádzačoch nielen telekomunikačných operátorov. Typové označenie PN-9108 označuje, že tento model má 8 napájaných výstupov typu IEC 60320/C13 Female a jeden vstupný konektor typu IEC 60320/C14 Male, ktorý napája ako celé zariadenie, tak aj výstupné konektory, pričom každý z týchto výstupov je užívateľmi ovládateľný. Maximálna celková zaťažiteľnosť sústavy udávaná výrobcom je 2300W. Ako sme si zvykli aj v predošlých dvoch prípadoch, spotreba samotného ATENU PN-9108 je veľmi nízka. Pohybuje sa na úrovni 10 až 12 Wattov bez pripojených spotrebičov. Spotrebiče sa pripájajú prepojovacím 3 pinovým PC káblom na 230V.



Obr. 11: Schéma zapojenia zariadenia ATEN PN-9108

ATEN PN-9108 sa ovláda podobne ako iné zariadenia od tohto výrobcu. Nastavovanie sa vykonáva prostredníctvom webového rozhrania, telnetu alebo sériového rozhrania. Prvotné prihlásenie je možné cez IP adresu 192.168.0.60.

V prípade nedostupnosti tejto IP adresy je možné IP adresu prideliť prostredníctvom DHCP servera. Prihlasovacie meno je administrator a heslo password. Všetky tieto údaje je možné po prihlásení sa oprávneniami správcu zmeniť. V prípade akýchkoľvek problémov je možné zariadenie ATEN KH-1516i vrátiť do výrobných nastavení. Jedným zo spôsobov je vykonať reset zariadenia cez webové rozhranie. V prípade, že IP adresu KVM prepínača nevieme, prepínač môžeme resetnúť cez mikro tlačítko na prednom paneli. Správu výstupných portov je možné prideliť jednotlivým, navzájom oddeleným užívateľom. Tieto výstupné napájacie porty je tiež možné vkladať do jednotlivých skupín. V prípade, že na ATEN PN-9108 máme pripojené zariadenia s väčšou spotrebou je odporúčané využiť funkciu oneskoreného zapínania pre prípad obnovenia napájania. Týmto môžeme predísť prípadnému špičkovému preťaženiu elektrickej sústavy. Azda neoddeliteľnou funkciou je možnosť pripojenia záložného zdroja v možnosti monitorovania stavu batérie. Táto funkcia spolupracuje s doplnkom Safe Shutdown a Reboot, ktorá v prípade kritického stavu batérie pošle signál pripojeným zariadeniam na vypnutie.



Obr. 12: Vzorové zapojenie stanice s použitím funkcie Safe Shutdown and Reboot

Tieto zariadenia sa tým pádom stihnú bezpečne vypnúť ešte pred tým, ako sa záložný zdroj úplne vybije. Týmto vieme zabezpečiť ochranu našich dát pred stratou ako sa stáva v prípade náhodného, alebo nečakaného vypnutia, čo určite neprospieva životnosti pevných diskov. Model so 110V napájacím napätím nám ďalej poskytuje ochranu voči preťaženiu na každý napájací port jednotlivo aj s nasledovnou obnovou napájania. Pre model s 230V napájaním je ochrana proti preťaženiu zabezpečená na všetky napájacie výstupy spoločne. Samozrejmosťou je aj časové ovládanie napájacích výstupov podľa vopred nastaviteľných intervalov. Za pomoci tejto funkcie vieme napríklad nastaviť to, aby fungoval niektorý z routrov len počas pracovnej doby, čím aj niečo môžeme ušetriť na celkovej spotrebe sústavy.

Veľkou výhodou zariadení z rady Pover over NET je možnosť ovládať pripojené spotrebiče cez internet. Výhodné to je aj v prípade nutnosti fyzického reštartu zariadení. ATEN PN-9108 a jemu podobné zariadenia nachádzajú svoje využitie hlavne v dátových rozvádzačoch firiem a telekomunikačných operátorov. Podľa mojich zistení, obdobné riešenia sú obľúbené hlavne menšími internetovými operátormi, ktorí si takto ovládajú jednotlivé zariadenia na prístupových bodoch. V prípade, že sa jedná o jednoduchšie riešenie, s obľubou sa používajú takzvané GSM reštartéry. Niektoré z nich už pracujú aj na IP vrstve a ich ovládanie je veľmi podobné, ako v prípade zariadení od ATENU.

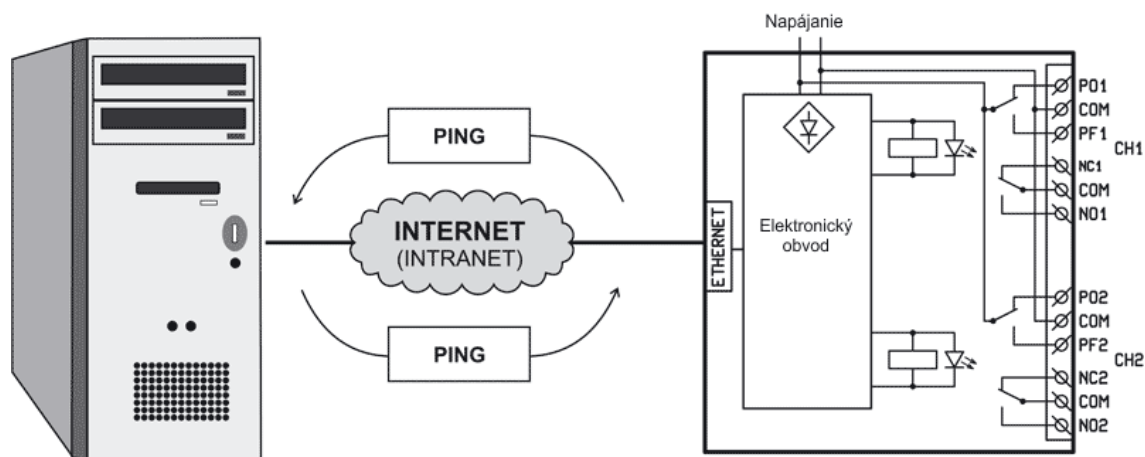
Medzi veľmi rozšírené možnosti dohľadu nad napájacími uzlami telekomunikačných sietí je použitie takzvaných Smart USP. Jedná sa o záložné zdroje, zväčša online záložné zdroje, ktoré zabezpečujú nepretržité napájanie prvkov telekomunikačnej siete v dátovom rozvádzači, alebo v dátovom centre. Tieto záložné zdroje sú zväčša osadené modulmi na vzdialený manažment obvykle cez rozhranie Fast Ethernet, alebo sériové rozhranie. Tieto moduly umožňujú nielen monitorovať prevádzku, ale do nej aj patrične zasahovať. Takéto kombinácie dohľadu sú s obľubou využívané telekomunikačnými operátormi, ktorí si dáta získané za pomoci týchto modulov nechávajú posielat' na centrálny dispečing, kde sa tieto telemetrické dáta nepretržite sledujú. Dáta sa posielajú väčšinou cez protokol SNMP, alebo sa v prípade kritických stavov zasielajú rovno SNMP Trapy. Jedná sa o výpadky elektriny, kapacitu a teplotu batérií, celkové zaťaženie a podobne. Na základe analýzy týchto dát pracovníci dispečingu vedia vyhodnotiť potrebné úkony na zachovanie nepretržitej prevádzky telekomunikačných zariadení.

Niektoré záložné zdroje umožňujú podobný rozsah funkcionality, ako je tomu aj v prípade použitia zariadení Power Over the NET od ATENU. To znamená, že sme schopní nastaviť oneskorené zapínanie jednotlivých napájacích výstupov, alebo ich reštartovať v prípade poruchy na telekomunikačnom zariadení. Oproti špecifickým zariadeniam, ako sú zariadenia Power Over the NET pociťujeme značné nedostatky rozsahu vytvárania nezávislých užívateľských účtov, nakoľko toto riešenie nie je určené pre koncových užívateľov, skôr na hrubý manažment napájacej sústavy v dátových rozvádzačoch, alebo dátových centrách v kombinácii so zabezpečením nepretržitého napájania. V prípade kombinácie s inými zariadeniami sme schopní v prípade identifikácie výpadku napájacieho napätia poslať príkaz na naštartovanie elektrocentrály. Na tento účel sa používajú smart boardy a analógovými, alebo digitálnymi vstupmi a výstupmi. Tieto výstupy nám cez elektronické obvody vedú ovládať štartér elektrocentrály.

V prípade, že nám sieťová infraštruktúra z nejakého dôvodu neumožňuje najideálnejšie pripojenie dohľadových zariadení, odporúča sa využívanie doplnkových funkcií na telekomunikačných zariadeniach akým je napríklad funkcia watchdogu. V preklade strážneho psa, ktorý je už integrovaný do väčšiny telekomunikačných zariadení buď softvérovo alebo hardvérovo. Táto doplnková funkcia chýba funkčnosť prevádzky telekomunikačných zariadení tak, že v prípade dosiahnutia nastavených podmienok vykoná reštart zariadenia, alebo iný nadefinovaný úkon. Môžeme nadefinovať funkcie kontroly dostupnosti služieb, alebo iných zariadení v sieti prostredníctvom protokolu ICMP. V prípade nedostupnosti nejakého zariadenia v sieti a po uplynutí vopred definovanej doby, bude vykonaný automatický reštart zariadenia. Táto funkcia sa hlavne využíva na miestach s problematickým napájaním, kde v prípade zakolísania napájacieho napätia zariadenia zamrzajú. Väčšinou sa stane, že zablokuje samotný napájací zdroj v zariadení, alebo prestane reagovať operačný systém. Pre posledný prípad sa odporúča využitie hardvérového watchdogu, ktorý je plne nezávislý od chodu operačného systému. Pri tomto prevedení by sa nemalo stať, že znefunkčnenie operačného systému odstaví aj funkcionality watchdogu.

Určité odrody watchdogov sa využívajú aj u prevádzkovateľov káblových a IP televízií. Tieto dohľadové zariadenia boli zväčša analógové a ich princíp sa zakladal na sledovaní napätíovej úrovne zvukového kanálu z danej ústredne. V prípade, že sa po dobu približne troch minút neobjavil zvuk na danom programe, zariadenie obsluhujúce

tento program bolo automaticky reštartované. V súčasnej dobe masívneho prechodu na digitálne vysielanie sa používajú sofistikovanejšie riešenia, ktoré nám prinášajú širšie spektrum možností. Digitálne spracovanie nám prináša možnosti kontroly kvality obrazu a v prípade výpadku sa moderné dohľadové systémy postarajú aj o automatické zálohovanie signálu z ďalšieho zdroja. Zaujímavé riešenie nám ponúka napríklad Scientific Atlanta, alebo Cisco Systems, ktorí ponúkajú špeciálne dohľadové servery pre vzdialenú správu ich zariadení. Tieto systémy môžeme prirovnať ku KVM prepínačom, Serial Over the NET, alebo Power Over the NET zariadeniam.



Obr. 13: Príklad použitia Watchdogu a jeho vnútorné zapojenie

4 Výsledok práce na zariadeniach ATEN

Výsledkom mojej bakalárskej práce je návrh laboratórnej úlohy pre účely predmetu KARS, ktorá tvorí časť prílohy. Úloha sa zaoberá použitím aktívnych prvkov pre vzdialený dohľad nad sieťovými zariadeniami. Pri laboratórnej úlohe budú použité vyššie spomínané zariadenia KH-1516i, SN-0116 a PN-9108. Cieľom úlohy nie je prinútiť študentov naučiť sa narábať výlučne so zariadeniami jedného výrobcu, ale priblížiť im použitie prvkov pre vzdialený dohľad v rámci reálnej prevádzky. V úlohe si vyskúšame vzdialenú správu a dohľad nad serverom za pomoci KVM prepínača a vzdialenej správy napájania, pričom si tiež overíme vzdialenú správu manažovateľného prepínača cez sériové rozhranie. Laboratórna úloha je navrhnutá tak, aby si študenti mohli overiť možnosti a prínos redundantného pripojenia na dohľadové zariadenia. Samotnú funkcionálnu redundanciu bude zabezpečovať smerovač Mikrotik, ku ktorému bude pripojený primárny okruh cez Ethernet a záložný okruh cez WiFi, alebo GSM sieť. V rámci tohto pokusu sa študenti tiež dozvedia, aké sú kapacitné nároky na prevádzkovanie jednotlivých dohľadových zariadení vzhľadom na počet súčasne pripojených užívateľov. Na základe tohto zistenia je možné posúdiť, či je možné na tieto účely použiť mobilné pripojenie, a keď áno, tak v akom rozsahu je toto možné.

5 Záver

Zo spracovaných informácií môžeme jednoznačne určiť, že zariadenia KVM, Serial over NET a Power over NET sú nevyhnutnou výbavou každého telekomunikačného operátora, ktorý to s poskytovaním siete a služieb myslí vážne. Najväčšiu efektivitu využitia týchto zariadení môžeme dosiahnuť vtedy, keď na tieto zariadenia bude pripojená internetová konektivita od iného operátora pre prípad výpadku internetovej konektivity v našej sieti. Toto riešenie umožní oživenie prevádzky našej siete a služieb aj vtedy, keď sme výpadok zapríčinili napríklad nedbalou konfiguráciou niektorého z našich hraničných smerovačov, alebo agregáčnych prepínačov. Zo skúseností aj od iných operátorov viem, že tieto zariadenia neslúžia len na zefektívnenie správy zariadení v sieti, ale pri správnom využití zvyšujú celkovú dostupnosť služieb ku spokojnosti všetkých koncových zákazníkov.

Podľa testov sme zistili, že na vzdialenú správu zariadení pomocou vzdialenej konzoly, alebo vzdialeného ovládania napájania, bude stačiť vo väčšine prípadov aj pripojenie cez mobilnú sieť. Pri pripojení cez mobilnú sieť už len z dôvodu rýchlejšej odozvy odporúčam pripojenie od operátora s dostupnou 3G sieťou. Vzhľadom k tomu, že tieto zariadenia majú slúžiť na odvrátenie výpadkov, odporúčame pripojiť tieto zariadenia na zabezpečenú internetovú konektivitu, alebo na nezávislé internetové pripojenie od iného poskytovateľa. Samozrejme na trhu sú dostupné aj zariadenia od iných výrobcov, ktoré sa cenovo ani funkčnosťou veľmi nelíšia. Dokonca sa často stretávame aj s tým, že samotné web rozhranie je okrem loga a farebných odtieňov úplne rovnaké. Avšak po dlhom testovaní a skúšaní môžeme skonštatovať, že zariadenia ATEN KH-1516i, ATEN SN-0116 a ATEN PN-9108 sú nesmierne robustným riešením pre akýkoľvek projekt, alebo aplikáciu a môžeme ich len vrelo odporúčať.

Počas testov sa tieto zariadenia javili veľmi stabilne a funkcie, ktoré sme od nich očakávali sa splňali na 100 percent. Veľkou výhodou týchto zariadení od spoločnosti ATEN je aj ich nízka spotreba a škálovateľnosť, čo je nezanedbateľné hlavne pri dlhodobej prevádzke. K väčšine týchto zariadení výrobca dodáva rozširovacie moduly a iné príslušenstvo podľa výberu, ktorými môžeme potenciál týchto zariadení ešte viac využiť. Pri výbere zariadení je dobré si overiť možnosti integrácie do dohľadového systému a podporu protokolov, akým je napríklad SNMP. Často sa stáva, že aj renomovaný výrobca podporuje sofistikovaný protokol na softvérový dohľad, čo

väčšinou znamená navýšené náklady. Na základe získaných vedomostí som vypracoval i laboratórnu úlohu, ktorá má študentom čo najviac priblížiť praktickú využiteľnosť daných zariadení a samotnej technológie vzdialeného dohľadu nad uzlami telekomunikačnej siete.

Použitá literatura

- [1] ATEN – manuály k ATEN KH-1516i, ATEN SN-0116 a ATEN PN-9108, 2010
- [2] Howe, B. *KVM Switch* [online]
Dostupný na URL: <http://en.wikipedia.org/wiki/KVM_switch>
- [3] Internetový portál Mikrotik, *The Dude 4 Documentation* [online]
Dostupný na URL: <<http://www.mikrotik.com/pdf/dude4.pdf>>
- [4] Internetový portál Wikipedia, *RMON* [online]
Dostupný na URL: < <http://en.wikipedia.org/wiki/RMON>>
- [5] NAGIOS - *Nagios Core Version 3.x Documentation* [online]
Dostupný na URL: <<http://nagios.sourceforge.net/docs/nagioscore-3-en.pdf>>
- [6] SOSINSKY, B. *Mistrovství - Počítačové sítě*. Computer Press, ISBN 9788025133637, ČR, 2010
- [7] Thomas, M. *Zabezpečení počítačových sítí bez předchozích znalostí*. CP Books, ISBN 80-251-0417-6, ČR, 2005
- [8] Wendell, O. *Směrování a přepínání sítí*. Computer Press, ISBN 978-80-251-2520-5, ČR, 2010

Zoznam príloh

Príloha č.1: Návrh laboratorní úlohy

Príloha č.2: Rozširovacie moduly k zariadeniu ATEN KH-1516i

Príloha č.3: Zapojenia prepojovacích káblov určených pre ATEN SN-0116

Príloha č.4: Schéma rádio modemovej siete s web rozhraním modemu Ripex

Prílohy

Návrh laboratorní úlohy

1 Cíl úlohy

Seznámení se zařízeními ATEN KH-1516i, ATEN SN-0116 a ATEN PN-9108 a poznání možností vzdáleného dohledu.

2 Seznam přístrojů a pomůcek

- ATEN KH - 1516i (KVM Over the NET)
- ATEN SN – 0116 (Serial Over the NET)
- ATEN PN – 9108 (Power Over the NET)
- Rozšiřovací modul KA9520 k zařízení ATEN KH-1516i
- Dvě pracovní stanice s OS Windows, jedno s připojením přes WiFi
- Switch se sériovým rozhraním
- Přednastavený Mikrotik Router s WiFi, nebo GSM rozhraním
- Schéma zapojení sítě
- Program IP Installer (je ke stažení i ze stránek výrobce)

3 Zadání úlohy

Seznamte se zařízeními ATEN KH-1516i, ATEN SN-0116 a ATEN PN-9108. Po podrobnějším prostudování nastavte jednotlivé zařízení podle zadání. Zařízení sestavte podle přiloženého schématu.

- 1 Router Mikrotik s WiFi nebo GSM rozhraním připojte sériovým kabelem DB9 - F na Serial Over The NET a jeho napájecí adapter připojte na Power Over The NET.
- 2 Server s windowsem a předinstalovanou aplikací IP Installer připojte na Power Over the NET a KVM. Nezapomeňte připojit i sériový kabel pro funkci Safe Shutdown and Reboot
- 3 Z důvodu ověření možností redundance se připájejte přes Ethernetovou síť i přes WiFi nebo GSM

- 4 Vyzkoušejte si přístupy přes různé přístupové účty na jednotlivé zařízení. Pro tento účel připojte manažovatelný přepínač se sériovým rozhraním. Po připojení zkontrolujte předepsanou přenosovou rychlost sériového rozhraní přepínače.
- 5 Se zvýšenou opatrností vyzkoušejte funkci Safe Shutdown and Reboot. Před zahájením procesu ověřte, zda je tento program nainstalovaný a či správně běží služba UPS ve windowse. V opačném případě může dojít během testu k poškození serveru.

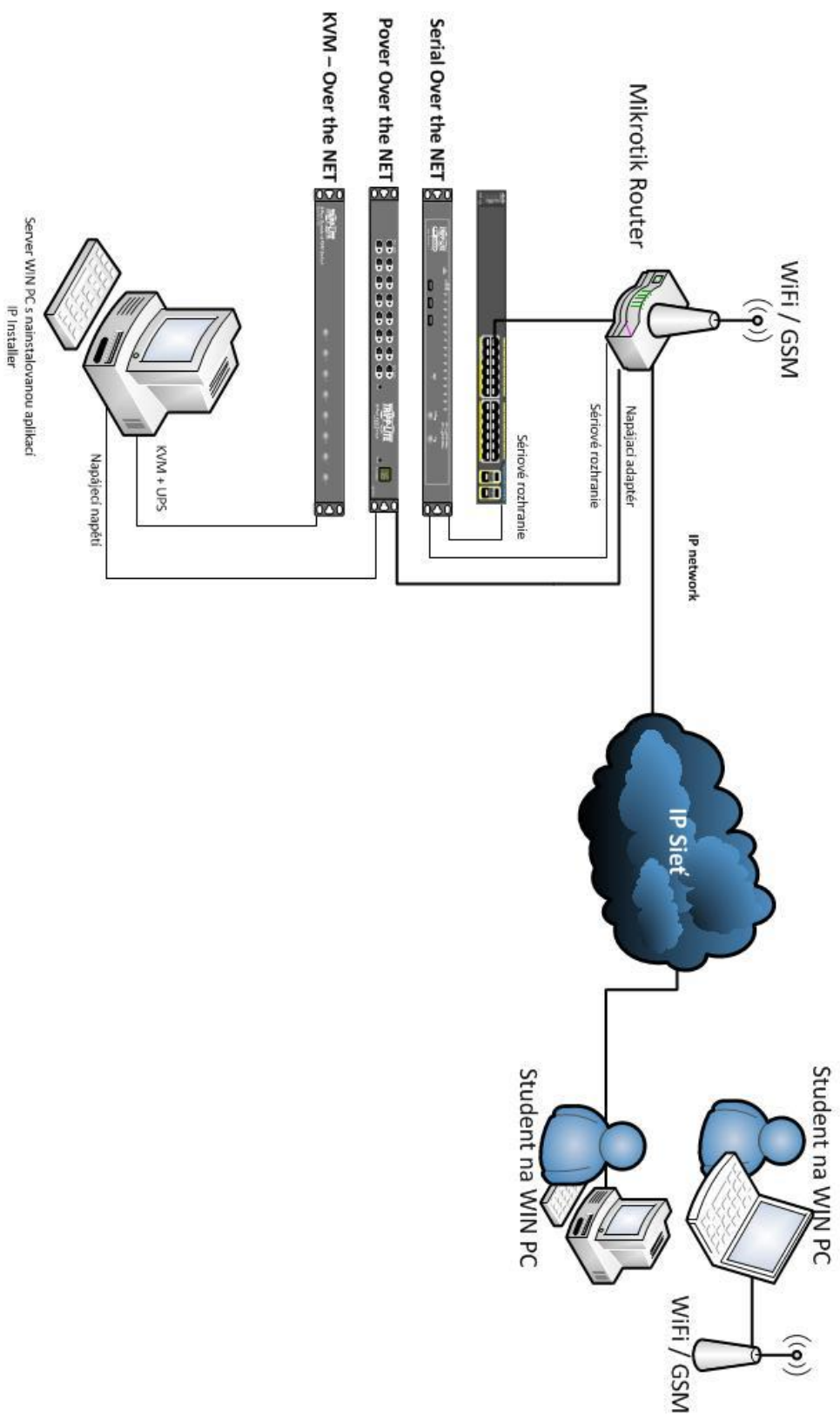
Přístupové údaje do jednotlivých zařízení:

Power Over the NET – IP 192.168.110.192, jméno/heslo: student1, student2

Serial Over the NET – IP 192.168.110.191, jméno/heslo: student1, student2

KVM Over the NET – IP 192.168.110.190, jméno/heslo: student1, student2

Mikrotik – IP 192.168.100.100, jméno/heslo: student1

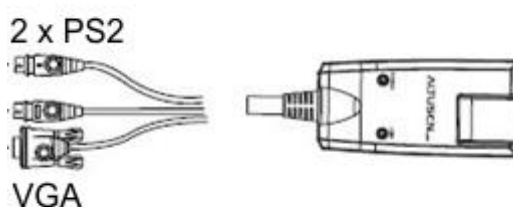


Obr. 1: Schéma zapojení zařízení k laboratorní úloze

4 Teoretické poznatky

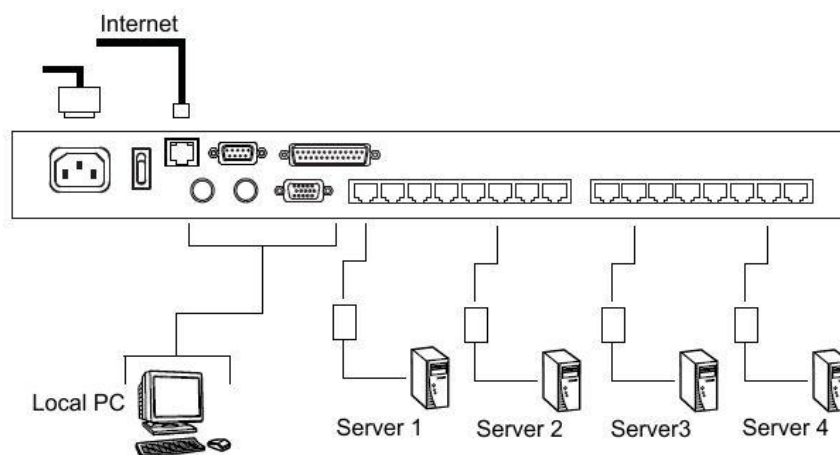
KVM Over the NET

Všechna důležitá nastavení jsou ovladatelná prostřednictvím webového rozhraní zařízení. ATEN KH-1516i je KVM přepínač, který nám umožňuje připojení jednotlivých zařízení za pomoci rozšiřujících modulů, které dodává výrobce a jsou dostupné i v naší laboratorní úloze. V úloze budeme používat modul KA9520, který nám umožní připojení klávesnice PS/2, myši PS/2 a monitoru VGA nebo SVGA.



Obr. 2: Rozšiřující modul KA9520 k zařízení ATEN KH-1516i

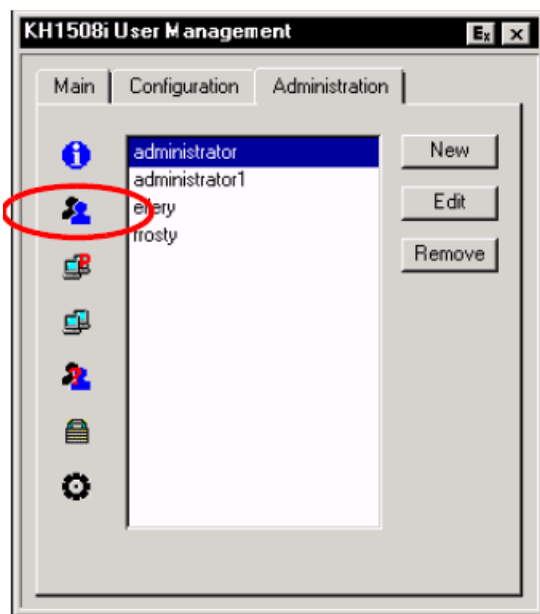
Modul se ke KVM přepínači připojuje přes kabel s konektorem RJ45, jejichž maximální délka je 30 až 40 metrů, závislá na rozlišení obrazu. Samotný KVM přepínač můžeme konfigurovat i lokálně za pomoci přímo připojeného monitoru, klávesnice a myši. Tento způsob konfigurace si můžeme vyzkoušet, ale pro splnění úlohy vykonáme konfiguraci přes webové rozhraní.



Obr. 3: Ilustrační zapojení KVM přepínače ATEN KH-1516i

Výchozí IP adresa KVM přepínače je 192.168.110.190. Přihlašovací jméno je **administrator** a heslo je **password**. Po přihlášení vidíme, že připojené zařízení můžeme ovládat přes klienta JAVA nebo přes klienta Windows.

Klient Windows je dostupný ke stažení přímo z webového rozhraní KVM přepínače. Klient Windows nám umožní kompletní konfiguraci zařízení, která je přehlednější jako webové rozhraní.

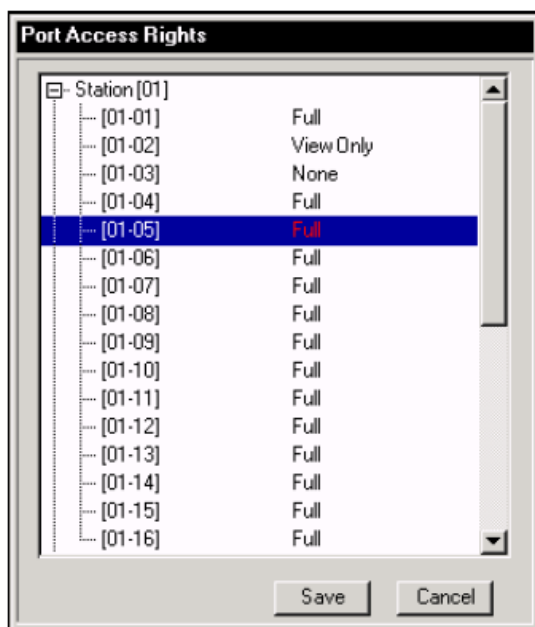


Obr. 4: Nastavení uživatelských účtů přes Win klienta na zařízení ATEN KH-1516i



Obr. 5: Přidávání uživatelských účtů přes Win klienta na zařízení ATEN KH-1516i

Správci zařízení se nastavuje oprávnění Admin, který tímto pověřením dostává plnou moc nad ovládáním každého připojeného zařízení. Pro vyšší bezpečnost můžeme nastavit oddělené uživatelské účty s oprávněním User.



Obr. 6: Nastavení oprávnění na jednotlivé výstupy přes Win klienta na zařízení ATEN KH-1516i

V položce Port Access Rights nastavíme oprávnění přístupů jednotlivých uživatelů na porty KVM přepínače. Kromě samotného povolení nebo zakázání přístupu na jednotlivé porty můžeme nastavit oprávnění na port pro daného uživatele jako View Only. Tento druh oprávnění nám umožní sledovat aktivitu na obrazovce, ale neumožní nám nijak zasáhnout nebo změnit nastavení.

Serial Over the NET

ATEN SN-0116 slouží na vzdálený přístup k sériovému rozhraní až 16 zařízení. Konfigurovat zařízení můžeme prostřednictvím webového rozhraní, telnetu nebo přes ssh. Prvotní konfiguraci uděláme přes webové rozhraní. Přístup je přes IP adresu 192.168.110.191. Přihlašovací jméno je administrator a heslo je password. Po přihlášení vidíme úvodní stránku, která zobrazuje stav jednotlivých výstupů. Každý ze 16 výstupů je nezávisle konfigurovatelný. Nastavení parametrů na jednotlivé porty uděláme přes položku Port Config. Zde máme možnost nastavení přenosové rychlosti, parity a ostatních nastavení komunikačního rozhraní.

Port Property Settings	
Port ID:	COM2
Port Name:	COM2
Baud Rate:	9600 bps
Data Bits:	8 bits
Parity:	None
Stop Bits:	1 bit
Flow Control:	None
Enable Toggle DTR:	No
Online Detect:	DSR
Out CRLF Translation:	None
Suspend Character:	D
Operating Mode:	Console Management
Timeout:	3 min. (0:Disable)
Authorized Operators:	administrator
<input type="button" value="Update"/>	

Obr. 7: Nastavení komunikačního rozhraní na zařízení ATEN SN-0116

Po nastavení jednotlivých rozhraní je na řadě nastavení uživatelských oprávnění. Uživatelé se přidávají v položce Adding an Account. Po přidání přihlašovacího jména a přihlašovacího hesla můžeme z tabulky vybrat jednotlivé rozhraní, na kterém může přidávaný uživatel komunikovat.

User Information				
Username:			Comments:	
Password:			Reenter password:	
<input type="checkbox"/> Port Config Permission				
Enable	Port Number	Port Name	Tcp Port	Shared
<input checked="" type="checkbox"/>	COM2	COM2	5002	Yes
<input checked="" type="checkbox"/>	COM3	COM3	5003	Yes
<input checked="" type="checkbox"/>	COM4	COM4	5004	Yes
<input checked="" type="checkbox"/>	COM5	COM5	5005	Yes
<input checked="" type="checkbox"/>	COM6	COM6	5006	Yes
<input checked="" type="checkbox"/>	COM7	COM7	5007	Yes
<input checked="" type="checkbox"/>	COM8	COM8	5008	Yes
<input type="button" value="Add"/> <input type="button" value="Back"/>				

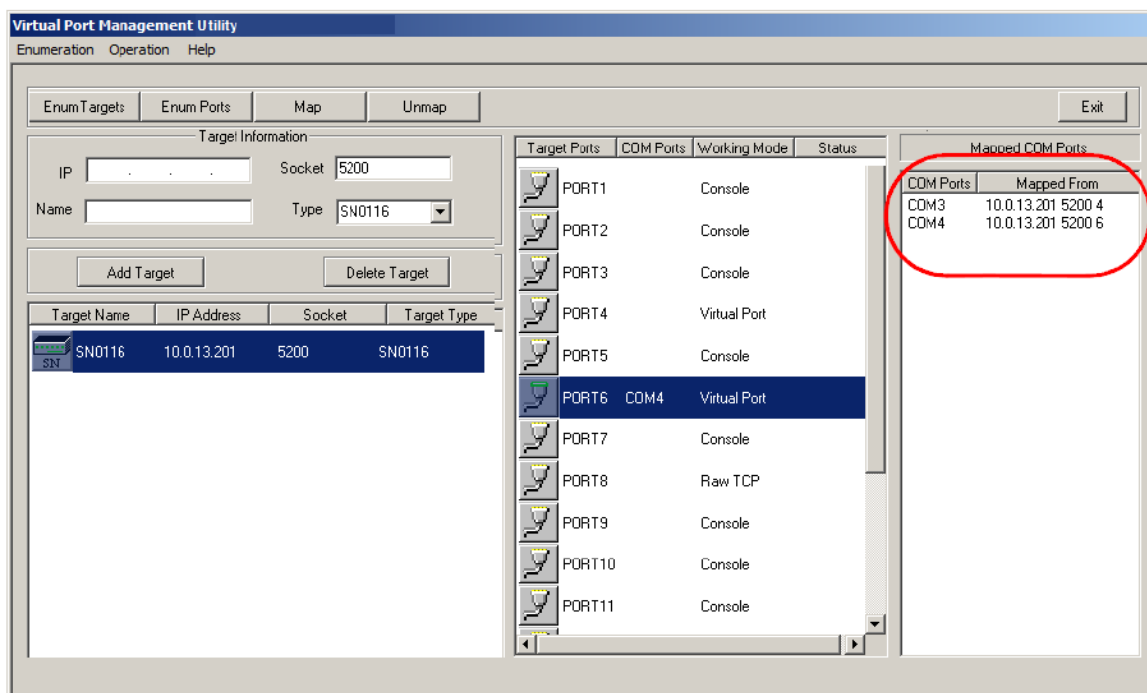
Obr. 8: Nastavení uživatelských účtů na zařízení ATEN SN-0116

Následně v položce Telnet Selection nastavíme TCP port pro jednotlivé rozhraní, za pomoci kterého budeme moci přímo přistupovat na sériové rozhraní námi zvoleného zařízení.

Telnet Selection			
Select	Port Number	Port Name	TCP Port
<input checked="" type="radio"/>	Local	-	23
<input type="radio"/>	COM2	COM2	5002
<input type="radio"/>	COM3	COM3	5003
<input type="radio"/>	COM5	COM5	5005
<input type="radio"/>	COM6	COM6	5006
<input type="radio"/>	COM7	COM7	5007
<input type="radio"/>	COM8	COM8	5008
<input type="radio"/>	COM9	COM9	5009
<input type="radio"/>	COM10	COM10	5010
<input type="radio"/>	COM11	COM11	5011
<input type="radio"/>	COM12	COM12	5012
<input type="radio"/>	COM13	COM13	5013
<input type="radio"/>	COM14	COM14	5014
<input type="radio"/>	COM15	COM15	5015
<input type="radio"/>	COM16	COM16	5016

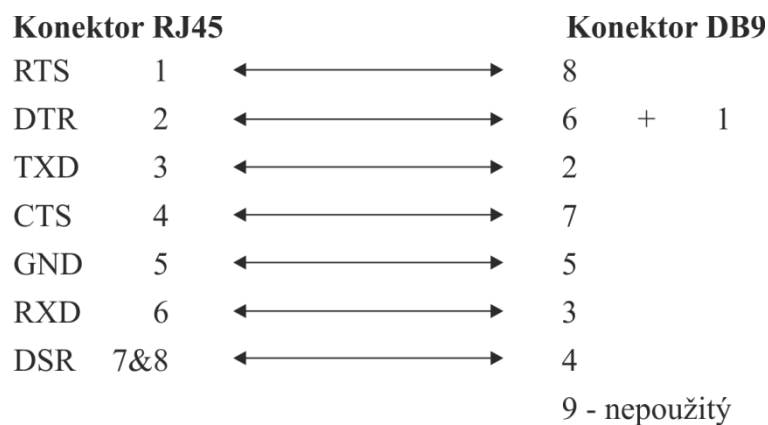
Obr. 9: Nastavení TCP portu na telnet přístup k jednotlivým rozhraním

Prostřednictvím aplikace Real COM Port Management, která je určená pro operační systémy Windows i Linux, můžeme vzdálený přístup na sériové rozhraní napamovat přímo na pracovním počítači jako virtuální sériové rozhraní, přičemž mapované rozhraní můžeme zabezpečit nastavením IP adres a portů. Aplikace Real COM Port Management je volně ke stažení ze stránek výrobce.



Obr. 10: Mapování virtuálního rozhraní na zařízení ATEN SN-0116 prostřednictvím aplikace Real COM Port Management

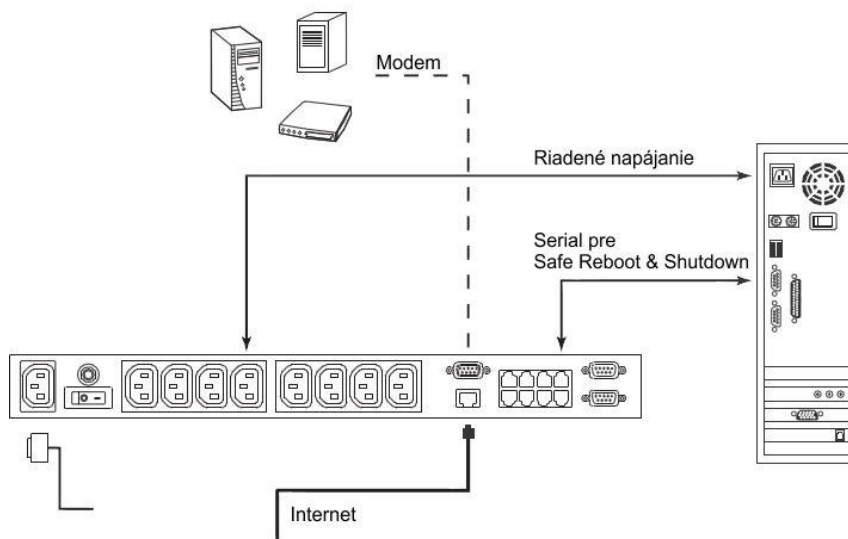
Na připojení zařízení je nutné použít propojovací kabely podle potřeby, kde jedna strana bude zakončená konektorem RJ45 a druhá konektorem DB9. Pro potřeby úlohy bude postačovat kabel RJ45-F - DB9-F, přičemž maximální délka kabelu by neměla být delší jak 15 metrů.



Obr. 11: Zapojení konektoru RJ45-F - DB9-F

Power Over the NET









ATEN PN-9108 slouží na dálkové ovládání napájení připojených zařízení. Zařízení se připojují přímo k ATEN PN-9108 prostřednictvím konektoru IEC 60320/C13 Female. Jednotlivé výstupy jsou plně ovladatelné a je možné je přidělovat do jedné ze čtyř skupin, pro jejich společné ovládání.



Obr. 12: Vzorové připojení stanic i s využitím funkce Safe Shutdown a Reboot

Konfigurace probíhá prostřednictvím webového rozhraní, telnetu nebo konzoly. Webové rozhraní, které nám umožní kompletní konfiguraci je dostupné pod IP adresou 192.168.110.192. Přihlašovací jméno je administrator a heslo je password.

Po přihlášení vidíme aktuální stav jednotlivých výstupů a skupin, které můžeme jednoduchým kliknutím zapnout nebo vypnout.

Power Status & Control					
Station: PN9108 - No.4			Current Load: 0.1 A		
A	 OFF <input type="checkbox"/> Reboot	Outlet-A Non Internet	E	 ON <input type="checkbox"/> Reboot	OutletE AC Back
B	 ON <input type="checkbox"/> Reboot	OutletB Kill Power	F	 OFF <input type="checkbox"/> Reboot	OutletF Kill Power
C	 ON <input type="checkbox"/> Reboot	OutletC Modem Ring	G	 OFF <input type="checkbox"/> Reboot	OutletG Modem Ring
D	 OFF <input type="checkbox"/> Reboot	OutletD Kill Power	H	 OFF <input type="checkbox"/> Reboot	OutletH Non Internet

Obr. 13: Stav výstupů na zařízení ATEN PN-9108

Zbarvení jednotlivých ikon znázorňuje stav dané zásuvky. Šedá ikona znamená, že zásuvka je vypnutá. Zelená ikona značí plně funkční a zapnutou zásuvku. Přechodové stavy, zapínání a vypínání, jsou označené blikající šedou a oranžovou ikonou. Doba vypnutí nebo zapnutí jednotlivých zásuvek záleží na aktuálním nastavení. Pro vypínání zásuvky je nastavitelné zpoždění minimálně 15 vteřin, které v kombinaci s funkcí Safe Shutdown and Reboot slouží k ochraně připojených stanic, které by se po zaslání vypínacího signálu měly vypnout. Takto by se mělo předejít ztrátě dat nebo poškození operačního systému na připojených stanicích.

Configuration							
Station: STATION_01 FW Ver: 1.0.093							
Station Name		STATION_01					
Outlet	Name	Modem Ring Resume	System after AC Back	Kill the Power	Confirmation Required	Power On Delay	Power Off Delay
A	OutletA	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>	0 sec	0 sec
B	OutletB	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>	0 sec	0 sec
C	OutletC	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>	0 sec	0 sec
D	OutletD	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>	0 sec	0 sec
E	OutletE	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>	0 sec	0 sec
F	OutletF	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>	0 sec	0 sec
G	OutletG	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>	0 sec	0 sec
H	OutletH	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>	0 sec	0 sec

Outlet Groups		
Group	Name	Outlets in Each Group
Group-1	Group-1	<input type="checkbox"/> A <input type="checkbox"/> E <input type="checkbox"/> C <input type="checkbox"/> D <input type="checkbox"/> E <input type="checkbox"/> F <input type="checkbox"/> G <input type="checkbox"/> H
Group-2	Group-2	<input type="checkbox"/> A <input type="checkbox"/> E <input type="checkbox"/> C <input type="checkbox"/> D <input type="checkbox"/> E <input type="checkbox"/> F <input type="checkbox"/> G <input type="checkbox"/> H
Group-3	Group-3	<input type="checkbox"/> A <input type="checkbox"/> E <input type="checkbox"/> C <input type="checkbox"/> D <input type="checkbox"/> E <input type="checkbox"/> F <input type="checkbox"/> G <input type="checkbox"/> H
Group-4	Group-4	<input type="checkbox"/> A <input type="checkbox"/> E <input type="checkbox"/> C <input type="checkbox"/> D <input type="checkbox"/> E <input type="checkbox"/> F <input type="checkbox"/> G <input type="checkbox"/> H

UPS Pin Assignments and Signal Polarities			
<input type="checkbox"/> Enable UPS			
Power Fail/Or Battery:	P6: CTS	<input checked="" type="radio"/> Negative	<input checked="" type="radio"/> Positive
Low Battery:	P1: DCD	<input checked="" type="radio"/> Negative	<input checked="" type="radio"/> Positive
UPS Shutdown:	P4: DTR	<input checked="" type="radio"/> Negative	<input checked="" type="radio"/> Positive
Warning! Please consult your UPS documentation before attempting to configure pin assignments and signal polarities.			
Save			

Obr. 14: Konfigurace výstupů s časováním na zařízení ATEN PN-9108

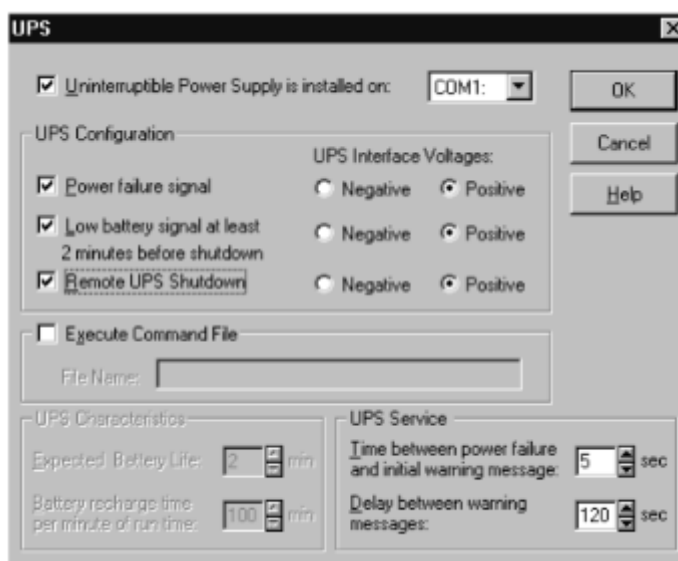
Power Off Delay umožňuje nastavení zpoždění při vypínání. Power On Delay slouží k nastavení zpoždění při zapínání. Výběrem Modem Ring Resume nastavíme zasílání term signálu, který slouží k oznámení vypínacího portu. Při kombinaci

s programem Program IP Installer se počítač bude moci bezpečně a včas vypnout. V opačném případě se po vypršení času zásuvka vypne bez upozornění. V položce Device Monitor vidíme celkové proudové zatížení na zařízení ATEN PN-9108.

Device Monitor								
ID	Name	Current Load	Outlet Status					
			A	B	C	D	E	F
01	PN9108-Station1	0.10 A						
02	CP0108RPSwitch	N/A						

Obr. 15: Monitorování proudového zatížení na zařízení ATEN PN-9108

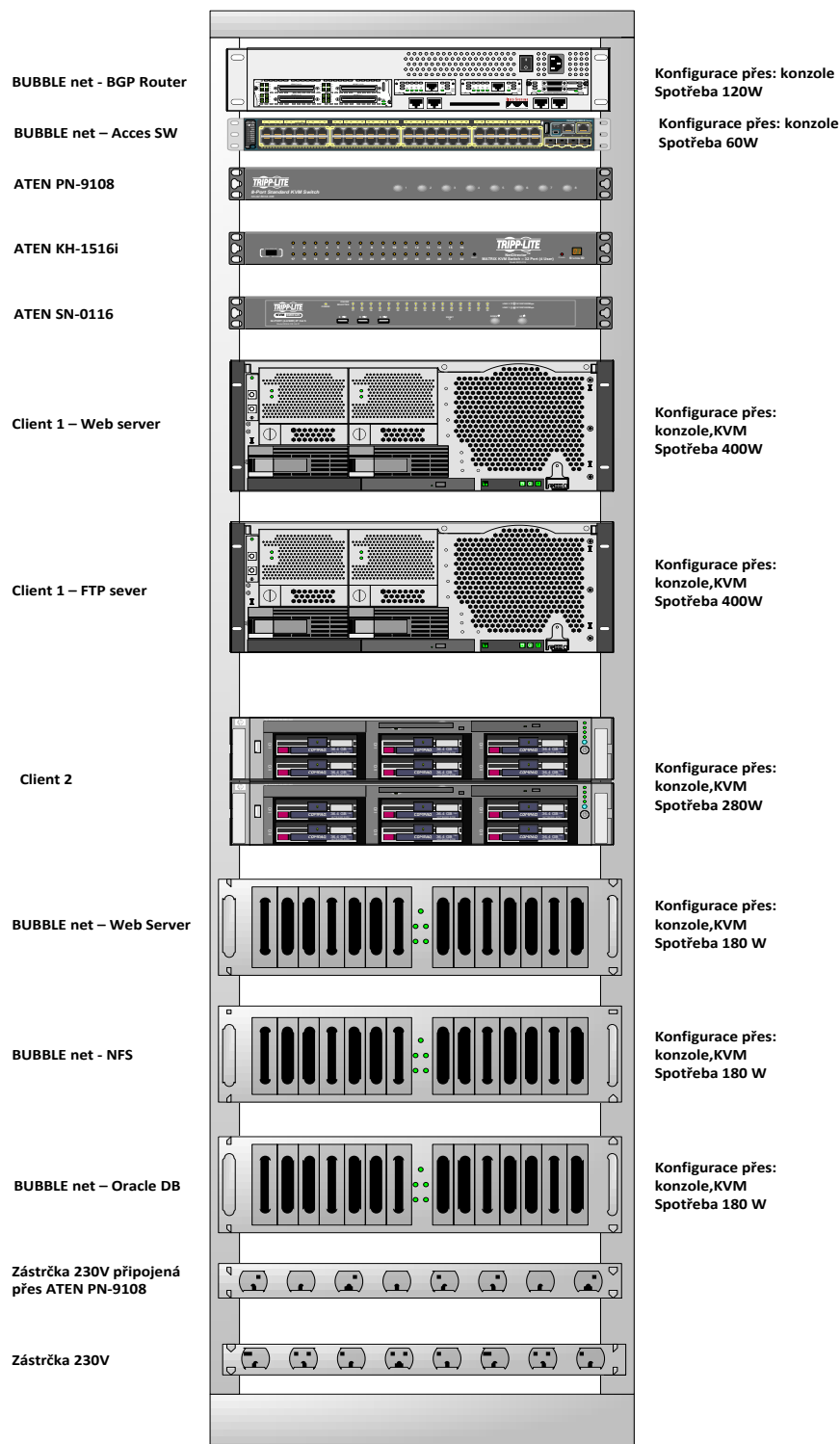
Program IP Installer je volně ke stažení ze stránky výrobce. Slouží ke komunikaci mezi ATEN PN-9108 a připojenými zařízeními prostřednictvím sériového rozhraní. Kabely ke komunikaci přes sériové rozhraní jsou v balení se zařízením ATEN PN-9108. Po instalaci programu se ve Windows přidá služba Uninterruptible Power Supply. Služba je totožná jako v případě připojení běžných záložních zdrojů. Nastavení aplikace IP Installer je velmi jednoduché a pravděpodobně ho po instalaci ani nebude nutné měnit.



Obr. 16: Nastavení aplikace IP Installer

5 Teoretická úloha

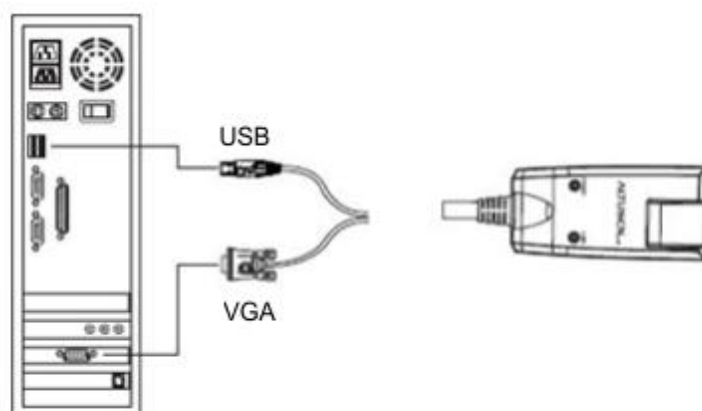
Úkol: Jak byste rozložili zátěž při připojení jednotlivých zařízení k Power Over the NET v rozváděči, aby nedošlo k vyřazení jističe v elektrickém rozváděči? Uveďte i důvod, proč tento jev nastává.



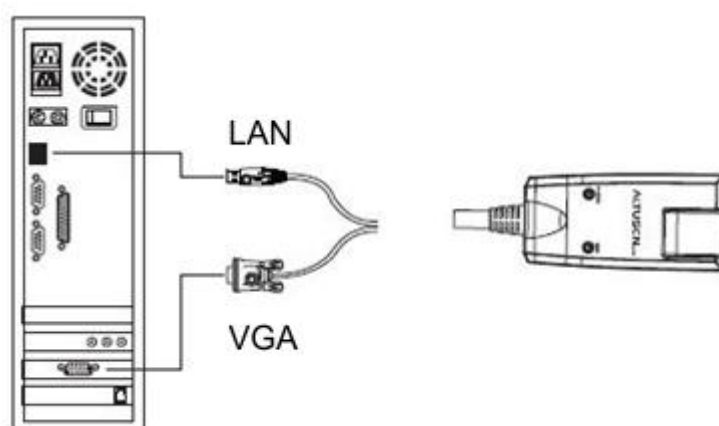
Obr. 17: Vzorový rozvaděč

Rozšiřovacie moduly k zariadeniu ATEN KH-1516i

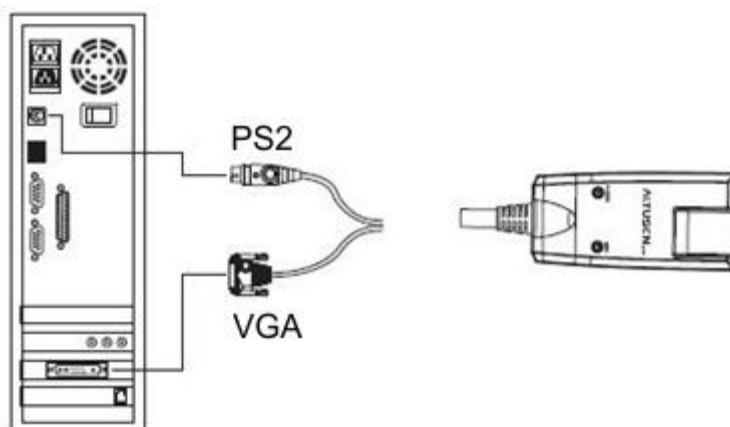
Zoznam rozšiřovacích modulov pre zariadenie ATEN KH-1516i



Obr. 1: Rozšiřovací modul KA9170 pre ATEN KH-1516i



Obr. 2: Rozšiřovací modul KA9570 pre ATEN KH-1516i



Obr. 3: Rozšiřovací modul KA9130 pre ATEN KH-1516i

Zapojenia prepojovacích káblov určených pre ATEN SN-0116

Konektor RJ45			Konektor DB9		
RTS	1	←→		7	
DTR	2	←→		4	
TXD	3	←→		3	
CTS	4	←→		8	
GND	5	←→		5	
RXD	6	←→		2	
DCD	7	←→		1	
DSR	8	←→		6	
					9 - nepoužitý

Obr. 1: Zapojenie prepojovacieho kábla RJ45-F - DB9-M pre ATEN SN-0116

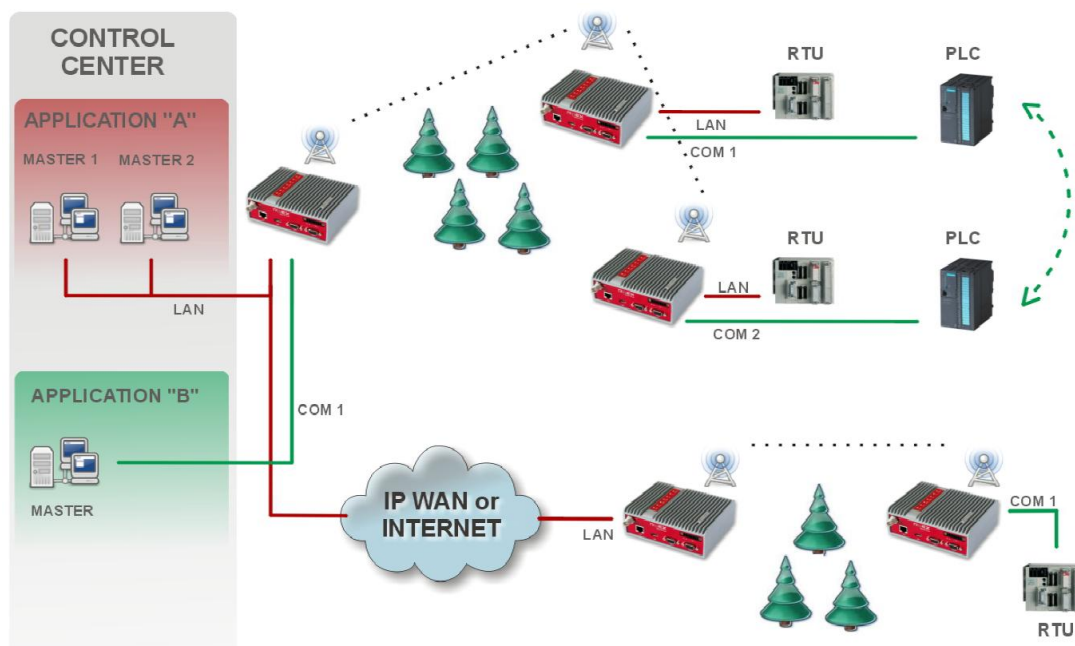
Konektor RJ45			Konektor DB25		
RTS	1	←→		5	
DTR	2	←→		6+8	
TXD	3	←→		3	
CTS	4	←→		4	
GND	5	←→		7	
RXD	6	←→		2	
DSR	7&8	←→		20	
					ostatné - nepoužíte

Obr. 2: Zapojenie prepojovacieho kábla RJ45-F - DB25-F pre ATEN SN-0116

Konektor RJ45			Konektor DB25		
RTS	1	←→		4	
DTR	2	←→		20	
TXD	3	←→		2	
CTS	4	←→		5	
GND	5	←→		7	
RXD	6	←→		3	
DCD	7	←→		8	
DSR	8	←→		6	
					ostatné - nepoužíte

Obr. 3: Zapojenie prepojovacieho kábla RJ45-F - DB25-M pre ATEN SN-0116

Schéma rádio modemovej siete s web rozhraním modemu Ripex



Obr. 1: Schéma zapojenia siete na báze rádio modemov RipEX od Racomu

The screenshot shows the web interface of a RipEX radio modem. The top header includes the 'RipEX' logo, the text 'Radio modem & Router', and the 'RACOM' logo. A sidebar on the left contains navigation links: Status, Wizards, Settings (highlighted), Routing, Diagnostic, Neighbours, Statistic, Graphs, Ping, and Maintenance. The main content area is titled 'Values from: ST 220' and features a 'Fast remote access' button. Below this, there are three main configuration sections: 'Device', 'Radio', 'ETH', and 'COM's'. The 'Device' section shows settings for 'Unit name' (ST 220), 'Time' (Manual), 'Alarm management' (Default), 'Power management' (Always On), and 'Neighbours&Statistics' (Default). The 'Radio' section includes settings for IP (10.10.10.222), Mask (255.255.255.0), TX frequency (402.100.000), RX frequency (402.100.000), RF power (0.2 W), Channel spacing (25.0 KHz), Modulation rate (83.33 | 16DEQAM), FEC (On (FEC 3/4)), Optimization (On), Encryption (AES 256), and MTU (1500). The 'ETH' section shows settings for IP (192.168.141.222), Mask (255.255.255.0), GW (192.168.141.254), DHCP (Off), Shaping (Off), Speed (Auto), Modbus TCP (Detail), and Terminal servers (Detail). The 'COM's' section shows settings for COM 1 and COM 2, including Type (RS232), Baud rate (19200 for COM 1, 38400 for COM 2), Data bits (8), Parity (None), Stop bits (1), Idle (5), MRU (1600), Flow control (RTS/CTS for COM 1, None for COM 2), and Protocol (Modbus for COM 1, DNP3 for COM 2). At the bottom, there are 'Apply' and 'Cancel' buttons. The footer contains copyright information for RACOM and the website URL www.racom.eu.

Obr. 2: Webové rozhranie na nastavenie parametrov rádio modemu RipEX od Racomu