



Středoškolská technika 2019

Setkání a prezentace prací středoškolských studentů na ČVUT

Monitorovací systém domácí sítě

Jakub Landa

Střední škola informatiky a finančních služeb

Klatovská 200 G, Plzeň

Prohlášení

Prohlašuji, že jsem svou práci SOČ vypracoval/a samostatně a použil/a jsem pouze prameny a literaturu uvedené v seznamu bibliografických záznamů.

Prohlašuji, že tištěná verze a elektronická verze soutěžní práce SOČ jsou shodné.

Nemám závažný důvod proti zpřístupnění této práce v souladu se zákonem č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších předpisů.

V Plzni dne 13. 5. 2019

Jakub Landa

Poděkování

Rád bych poděkoval mému vedoucímu práce panu Mgr. Bc. Petru Zimovi za odborné vedení a rady při zpracovávání této práce.

Dále bych pak chtěl poděkovat paní Mgr. Lucii Martínkové za cenné rady, věcné připomínky a vstřícnost při konzultacích prezentace a písemné části práce.

Anotace

Tato práce se zabývá vytvořením sledovacího systému domácí sítě, který slouží k sledování předem daných zařízení a jejich vzdálené správě. Dále se také zabývá popsáním protokolu SNMP a funkce Wake on LAN spolu s jejich využitím ve firemním prostředí.

Prvním cílem bylo vytvořit SNMP server, který by získával informace a ukládal je do databáze.

Dalším cílem bylo vytvoření webových stránek, do kterých by se promítala data z databáze a na kterých by se nacházel ovládací panel pro vzdálenou správu spolu s funkcí automatického zapínání počítače na základě před dané události.

Oba cíle se mi podařilo splnit.

Klíčová slova

SNMP; Monitorování; Webové stránky; Vzdálená správa

Annotation

This work is focused on creation of monitoring system of home network, which is used for monitoring and remote management of predefined devices. It is also describing a SNMP protocol with Wake on LAN function along with their use in corporate environment.

First goal was to create a SNMP server, which would get informations and store them into database.

Next goal was to create a web pages for presenting acquired data from the databse and for remote management of predefined devices via web control panel. Control panel would also had a function of auto startup based on a predefined event.

I have managed to accomplish both goals.

Keywords

SNMP; Monitoring; Web pages; Remote management

Obsah

Úvod.....	7
1 Teoretická část – Protokol SNMP a standard Wake on LAN.....	8
1.1 Protokol SNMP.....	8
1.1.1 OID a MIB.....	8
1.1.2 Verze protokolu SNMP.....	9
1.1.3 SNMP dotazování.....	9
1.1.4 Způsoby využití SNMP pro monitorování zařízení.....	9
1.2 Standard Wake on LAN a jeho využití.....	10
1.2.1 Popsání chování Wake on LAN.....	10
1.2.2 Využití Wake on LAN.....	11
2 Aplikační část – Monitorovací systém domácí sítě.....	11
2.1 Popsání hardwarové části serveru.....	11
2.2 Popsání softwarové části serveru.....	12
2.2.1 SNMP server.....	12
2.2.2 Databáze.....	12
2.2.3 Webový server.....	12
2.2.4 Wake on LAN.....	13
2.3 Získávání informací od zařízení.....	13
2.4 Webové stránky pro ovládání systému.....	13
2.4.1 Zabezpečení stránek a domovská stránka.....	14
2.4.2 Monitorovací panel.....	15
2.4.3 Ovládací panel.....	16
2.4.3.1 Vzdálené spuštění a vypínání PC.....	17
2.4.3.2 Aktivní režim.....	18
2.4.3.3 Vzdálená plocha.....	19
2.4.3.4 Mobilní verze ovládacího panelu.....	19
Závěr.....	20
Přílohy.....	20
Příloha 1: Skript pro získávání a ukládání informací (dbscript.sh).....	20
Příloha 2: Skript pro aktivní režim (active.sh).....	23

Seznam použitých obrázků	24
Použité zkratky.....	24
Použité informační zdroje	24

ÚVOD

Cílem mého projektu bylo vytvoření monitorovacího systému domácí sítě, který by sloužil k zobrazování aktuálních informací o zařízeních v domácí síti a zároveň sloužil ke vzdálené správě stolního počítače nalézajícího se v domácí síti.

Motivací pro tuto práci pro mě byla zkušenost s prací v monitorovacím systému Check_MK při mé stáži na Krajském úřadě Plzeňského kraje v oddělení správy sítě a serverů. Zde jsem se dozvěděl o protokolu SNMP a jeho využití k monitorování zařízení. Jednoduchost protokolu mě nadchla a rozhodl jsem si vytvořit vlastní monitorovací systém, který by byl uživatelsky přívětivější a jednodušší než výš zmiňovaný Check_MK. Nápad pro zakomponování vzdálené správy mi pak vnukla odborná výuka na mé škole.

V teoretické části mé práce se zabývám stručným popsáním protokolu SNMP a jeho využití pro monitorování zařízení v internetových sítích. Dále zde pak popisuji standard Wake on LAN, primárně jeho fungování a využití.

Aplikační část mé práce pak tvoří podrobný popis veškerých důležitých částí monitorovacího systému od popisu hardwarového provedení serveru až po popis stylizace webových stránek pro různé typy zařízení.

V přílohách pak uvádím skripty použité pro chod hlavních funkcí monitorovacího systému.

1 TEORETICKÁ ČÁST – PROTOKOL SNMP A STANDARD WAKE ON LAN

V této části práce se budu věnovat stručnému popsání fungování protokolu SNMP a jeho využití pro monitorování stavu síťových prvků a serverů. Dále se pak zaměřím na standard Wake on LAN a jeho využití.

1.1 Protokol SNMP

SNMP neboli Simple Network Management Protocol je aplikační protokol plně definovaný v dokumentu RFC 1157.

Protokol slouží ke vzdálenému nastavování nebo sledování zařízení.

K fungování protokolu jsou zapotřebí manager a agent.

Manager je nástroj/software, který se dotazuje na stav zařízení, nebo zařízení nastavuje. Manager také může poslouchat na portu UDP 162 a sbírat Trap zprávy posílané agentem.

Agent je software, který běží na koncovém zařízení a poslouchá na portu UDP 161. Rolí agenta je odpovídat na dotazy managera, nebo automaticky posílat zprávy o svém stavu (Trap zprávy) managerovi.

1.1.1 OID a MIB

Data jsou pro SNMP prezentována v rámci stromové struktury posloupných číselných hodnot oddělených tečkou. Tyto hodnoty se nazývají OID (Object Identifier) a fungují jako proměnné. Do těchto proměnných jsou pak ukládány systémové hodnoty zařízení.

Např. OID obsahující verzi OS u routeru pak vypadá takto: .1.3.6.1.4.1.14988.1.1.4.4.0

Takto sestavená stromová struktura není pro člověka moc přehledná. Proto existují MIB databáze. MIB je zkratkou pro Management Information Base. Jedná se o seznam, který přeloží OID na lidsky čitelné názvy, podle kterých se lze lépe orientovat. Podrobná specifikace MIB je pak popsána v dokumentu RFC 1066.

Pro fungování SNMP však záleží pouze na OID. MIB je tedy pro funkčnost protokolu nepotřebné. Slouží pouze k lepší interpretaci hodnot.

Je důležité zmínit, že každý výrobce si může vlastní OID strukturu navrhovat sám. Z toho důvodu většina společností poskytuje ke svým výrobkům vlastní MIB databázi.

1.1.2 Verze protokolu SNMP

Protokol SNMP existuje ve třech verzích, a to ve verzi 1, 2c a ve verzi 3.

Verze 1 a 2c používají k ověřování takzvaný community string, což je název uskupení, do kterého sledovaná zařízení patří. V podstatě slouží jako textové heslo. Oproti verzi 1 se verze 2c liší hlavně tím, že obsahuje kontrolu doručení zprávy, takže by se nemělo stávat, že zpráva nedorazí. Dále pak obsahuje novou funkci pro dotazování get-bulk, která dokáže získat větší objem informací najednou.

Verze 3 pak nabízí převážně možnost autentizace skrze uživatelské jméno a heslo za využití MD5 nebo SHA hashování. Podstatnou změnou je také šifrování komunikace pomocí AES nebo DES šifrování.

1.1.3 SNMP dotazování

Dotazování v SNMP probíhá ze strany managera na agenta. Existuje několik typů dotazů pro získání dat.

Základním dotazem je snmpget. Tento dotaz vrátí pouze hodnotu OID, které je zadáno.

Příklad: `snmpget -v2c -c secure -Ov 192.168.20.1 .1.3.6.1.2.1.25.2.3.1.5.65536`

Dalším dotazem je pak snmpwalk, který vypíše buď celý stromový záznam, nebo vše co je níže ve stromové struktuře než OID, které je zadáno jako parametr.

Příklad výpisu celé stromové struktury: `snmpwalk -v2c -c secure -Ov 192.168.20.1`

Dalšími dotazy jsou pak snmpbulkget a snmpbulkwalk. Tyto dotazy mají stejnou syntaxi s výše uvedenými dotazy. Rozdílem je akorát větší obsah dat, který tyto dotazy získávají.

1.1.4 Způsoby využití SNMP pro monitorování zařízení

SNMP je dnes hojně využíváno ve firmách právě pro udržování přehledu o stavu síťových zařízení a serverů.

Firmy většinou používají komerční monitorovací systémy, které ale ve svém jádru využívají právě SNMP. Hlavní výhodou SNMP je jeho jednoduchost a široká podpora mezi výrobci prvků sítě a serverů.

Jedna z možností fungování monitorovacího systému je, že sám posílá dotazy a odpovědi si ukládá do databáze z které následně tvoří statistiky a grafy.

Druhá možnost je, že systém pouze v poslouchá a přijímá Trap zprávy, které jsou generované nakonfigurovanými agenty. Trap zprávy lze nakonfigurovat tak, aby odesílali jen například chybové hlášky.

Monitorovací systémy většinou používají obě dvě možnosti. První možnost využívají z důvodu souvislého uspořádání dat do časové osy. Možnost s přijímáním Trap zpráv pak využívají k získávání informací o chybách zařízení.

Každý systém se ale chová jinak a je hlavně na správci systému, jak se rozhodne data sbírat.

Ve firemních prostředích jsou velice rozšířené monitorovací systémy jako Zabbix, LibreNMS, Check_MK a Nagios. Všechny tyto systémy využívají právě protokol SNMP.

Jedná se velmi pokročilé systémy, které jsou velmi přizpůsobitelné. V praxi to pak vypadá tak, že administrátor systému má uspořádané určité typy zařízení do logických celků a jednotlivá zařízení ještě pospojovaná do logické mapy sítě. Na monitoru se mu pak budou zobrazovat kolonky typu routery, switche, servery atd. spolu s mapou zapojení daných zařízení. Většina těchto systému také nabízí funkce tvorby grafů ze sesbíraných dat.

Při přidávání nových zařízení do systémů to vypadá tak, že administrátor musí zadat IP adresu agenta, a v závislosti na verzi pak komunitu nebo uživatelské jméno a heslo. Systémy pak sami rozeznají, o jaký druh zařízení se jedná a interpretují data do přehledných tabulek či grafů. Systémy také často obsahují možnost přidání sledování určitého OID.

Monitorovací systém dne nechybí snad v žádné větší ani střední firmě či instituci. V dnešní době se jedná v podstatě o nutnost.

1.2 Standard Wake on LAN a jeho využití

Wake on LAN je Ethernetový standard, který vznikl v roce 1997 spoluprací firmy Intel a IBM.

1.2.1 Popsání chování Wake on LAN

Jedná se o standard používaný k zapnutí nebo probuzení počítače. Wake on LAN používá tzv. magic paket, který v sobě obsahuje MAC adresu zařízení, které má zapnout. Tento paket je rozeslán broadcastem v lokální síti. Počítač, který je vypnutý se ve skutečnosti nachází v režimu minimální spotřeby a na síťovém rozhraní dokáže přijmout právě magic paket. Když na takovýto počítač přijde magic paket a MAC adresa obsažená v magic paketu se shoduje s MAC adresou vypnutého počítače, tak počítač zahájí start jako kdyby uživatel zmáčkl startovací tlačítko.

Pro fungování Wake on LAN je ale zapotřebí podpory síťových karty a základní desky. Na základní desce s většinou musí Wake on LAN povolit. Povolení se provádí v BIOSu nebo UEFI, záleží na typu základní desky.

1.2.2 Využití Wake on LAN

Wake on LAN lze využít hlavně na vzdálené zapínání počítače nebo jiného síťového zařízení s podporou Wake on LAN. Uplatňuje se například při automatizovaném zapínání serverů či pracovních stanic. Široké využití také nachází v prostředí IOT, jelikož standard funguje pro bezdrátový přenos.

2 APLIKAČNÍ ČÁST – MONITOROVACÍ SYSTÉM DOMÁCÍ SÍTĚ

Jak jsem již psal, tato práce má za cíl vytvoření domácího monitorovacího systému sítě s možností vzdálené správy.

Úkolem systému je automaticky sbírat předem určená data o stavu domácího routeru, stolního počítače v domácím prostředí a data o serveru, na kterém systém běží. Tato data pak systém ukládá do databáze.

Jednou z nejpodstatnějších částí jsou webové stránky, přes které je celý systém prezentován uživateli. Stránky se skládají z dvou hlavních částí, a to je monitorovací panel a ovládací panel.

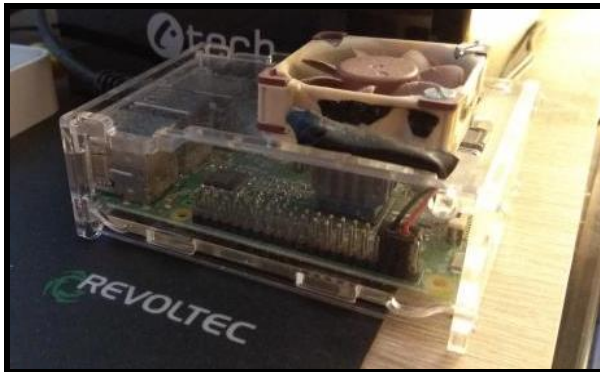
Monitorovací panel slouží k zobrazení aktuálního stavu sledovaných zařízení pomocí výpisu dat z databáze. Zobrazení a uspořádání dat v monitorovacím panelu bude podrobně popsáno až níže v dokumentu.

Ovládací panel pak slouží ke vzdálené správě stolního počítače. Vzdálená správa zahrnuje vzdálené vypnutí a zapnutí počítače, vzdálenou plochu počítače, tzv. Aktivní režim, který slouží k automatickému zapnutí počítače, když je splněna určitá podmínka, konkrétně příchod uživatel domů z práce/školy. Dále se v panelu nachází možnost vzdáleného restartu serveru a přístup do webového rozhraní správy databáze spolu s výčtem posledních šesti zapnutí a vypnutí stolního počítače s časem a datem, kdy se tak stalo. Podrobnější popis ovládacího panelu a jeho nejpodstatnějších funkcí bude opět rozebrán níže.

2.1 Popsání hardwarové části serveru

Jelikož systém má za úkol sledovat jen malý počet zařízení, nebylo potřeba extra výkonného stroje. Proto jsem pro účel serveru zvolil počítač Raspberry Pi 3 Model B z důvodu skladnosti a vynikajícího poměru cena/výkon. Počítač disponuje čtyřjádrovým ARM procesorem s frekvencí jádra 1.2 GHz a operační pamětí o velikosti 1 GB. Pro uložení operačního systému a dat je pak použita microSD karta. Počítač také disponuje zabudovaným 100 MB ethernetovým konektorem a wifi adaptérem. Z důvodu stability vyšší přenosové rychlosti je využit pouze ethernetový konektor.

Pro ochranu počítače jsem použil plastový kryt a pro udržení stabilních teplot jsem využil jak pasivního chlazení v podobě žebrového chladiče procesoru, tak i aktivního chlazení za použití ventilátoru.



Obrázek 1: Monitorovací systém – Server

2.2 Popsání softwarové části serveru

Na počítači je nainstalován operační systém Raspbian Stretch Lite. Jedná se o upravenou verzi linuxového operačního systému Debian přímo pro Raspberry Pi.

Verzi bez grafického rozhraní jsem zvolil převážně kvůli úspoře výpočetního výkonu a také z toho důvodu, že se serverem pracuji pouze skrze příkazové rozhraní.

2.2.1 SNMP server

Aby můj server fungoval jako SNMP manager využívám balíčku `snmp`.

Nainstalovat lze pomocí příkazu: `sudo apt-get install snmp`

Balíček `snmp` obsahuje funkce pro dotazování a nastavování SNMP agentů (`snmpget`, `snmpwalk`, `snmpset`) spolu s vlastností příjmu Trap zpráv.

2.2.2 Databáze

Pro roli databáze zde využívám svobodnou odnož MySQL databáze, a to databázi MariaDB. Zvolil jsem si jí z toho důvodu, že je jako výchozí volbou pro instalaci databáze na bázi MySQL v systému Raspbian. Od MySQL se liší akorát tím, že je dostupná pod svobodnou licenci, zatímco MySQL je vlastněna společností Oracle.

2.2.3 Webový server

K provozování webových stránek používám open-source Apache2 server, který jsem si zvolil kvůli jeho vysoké rozšířenosti a popularitě.

Server pro HTTPS šifrování využívá self-signed certifikát, aby nemohlo dojít k odcizení přihlašovacích údajů.

2.2.4 Wake on LAN

Pro funkci Wake on LAN využívám balíček etherwake, který po zadání parametrů pro odchozí síťové rozhraní a cílovou MAC adresu sestaví magic paket a odešle ho.

Nainstalovat lze pomocí příkazu: *sudo apt-get install etherwake*

Tuto možnost jsem zvolil převážně proto, že tento balíček je otestovaný a plně funkční, tudíž jsem se nemusel zatěžovat s psaním vlastního scriptu a mohl jsem se plně věnovat tvorbě webových stránek systému.

2.3 Získávání informací od zařízení

Informace jsou získávány dvojitým způsobem.

Z routeru a stolního počítače jsou informace získávány pomocí protokolu SNMP, konkrétně ve verzi 2c.

Verzi 2c jsem oproti verzi 3 zvolil proto, že jednodušší na nastavení. A jelikož systém operuje v prostředí domácí sítě, do které nemají přístup osoby zvenčí, je nasazení verze 2c dostačující.

Pro získávání informací o serveru samotném využívám interních linuxových příkazů z důvodu jejich větší přesnosti a možnosti lepší úpravy výstupu informací.

Veškeré získávání informací se ale děje pomocí jednoho bash skriptu. Skript se prvně pomocí pingu ujistí, že zařízení jsou zapnutá. Pokud ping proběhne v pořádku, tak si skript vytáhne informace o stavu zařízení pomocí SNMP či linuxového příkazu a uloží je do proměnných. Když ping selže, tak si skript do proměnných uloží informaci o tom, že zařízení je vypnuté. Jakmile si do proměnných uloží všechny hodnoty, tak začne s jejich ukládáním do databáze.

Skript je automaticky spouštěn každých 5 minut za využití plánovače cron, který je obsažen v operačním systému. Dále je pak také spouštěn každou minutu, pokud si uživatel zobrazuje monitorovací panel na webových stránkách.

2.4 Webové stránky pro ovládání systému

Webové stránky jsou prostředek, skrze který jsou uživatelům prezentována získaná data a možnosti vzdálené správy, které systém nabízí.

Abych mohl pomocí stránek provádět spouštění řídicích skriptů na serveru, rozhodl jsem se použít programovacího jazyka PHP, ve kterém jsem stránky psal.

K vytvoření webových stránek namísto programu např. v programovacím jazyce Java jsem se rozhodl z toho důvodu, že webové stránky jsou přístupné z většiny typů zařízení, ať se jedná o smartphone, notebook nebo stolní počítač. Hlavní výhodou je že uživatel nepotřebuje nic víc než webový prohlížeč.

U myšlenky přístupu z více zařízení jsem zůstal a navrhl jsem stránky ve verzi pro smartphone a pro notebook/stolní počítač.

Stránky se zobrazí ve správné verzi na základě rozpoznání rozlišení displeje zařízení.

Mobilní verze je uzpůsobená tak, aby byly zvýrazněny hlavně ovládací prvky. Nejvýraznější úprava pro mobilní verzi se týká hlavně ovládacího panelu.

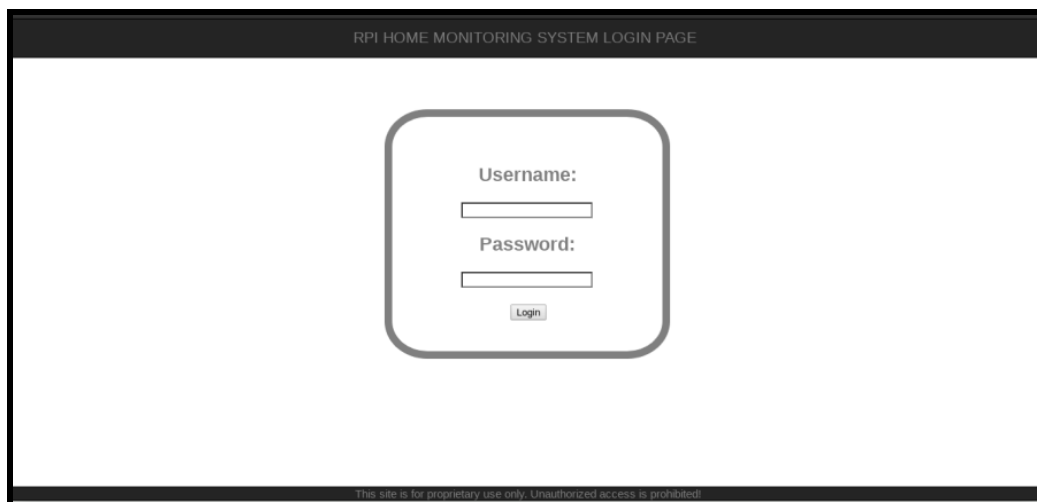
2.4.1 Zabezpečení stránek a domovská stránka

Jelikož pomocí systému lze ovládat fyzický počítač, je na místě zabezpečení přístupu do systému.

Jak jsem se již psal, přenos přihlašovacích údajů je chráněn pomocí šifrovaného protokolu HTTPS.

Ověření uživatele je zprostředkováno skrze přihlašovací stránku, a to porovnáním uživatelského jména a hesla s daty v databázi.

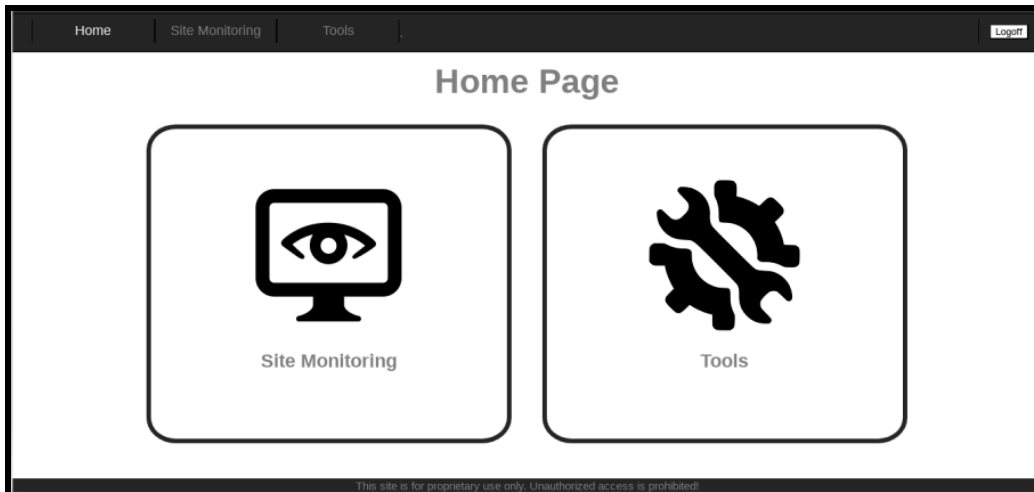
Přihlašovací stránka obsahuje dvě jednoduchá pole pro uživatelské jméno a heslo.



Obrázek 2: Monitorovací systém – Přihlašovací stránka

Po ověření je uživateli přiřazena PHP session ID, díky které systém pozná, že uživatel je autorizován ke vstupu. Uživatel je následně přesměrován na domovskou stránku.

Domovská stránka plní výhradně funkci rozcestníku mezi monitorovacím a ovládacím panelem.



Obrázek 3: Monitorovací systém – Domovská stránka

Každá část stránky si pak hlídá platnost session ID a pokud stránka zjistí neplatné ID, je uživatel přesměrován zpět na přihlašovací stránku. To zabraňuje možnosti, že by případný útočník chtěl přeskočit fázi ověření tím, že by zadal plnou cestu např. k ovládacímu panelu.

2.4.2 Monitorovací panel

Hlavní úlohou monitorovacího panelu je zobrazování aktuálních informací o běžících zařízeních.

Systém sleduje domácí router, stolní počítač a server, na kterém běží. Z toho důvodu jsou v monitorovacím panelu zobrazené tři tabulky. Všechna zařízení mají kolonku STATUS a UPTIME. Kolonka STATUS indikuje, jestli zařízení je zapnuté či nikoliv. Kolonka UPTIME pak říká, jak dlouho zařízení běží. Další kolonky pak jsou specifické pro dané zařízení. Například kolonka OS VERSION je pouze u routeru, jelikož se zde jedná o důležitou informaci. U stolního počítače pak taková kolonka chybí, jelikož není tak důležitá.

U routeru se sleduje status, doba běhu zařízení, verze operačního systému, vytížení paměti a využití úložiště.

U stolního počítače je sledován status, doba běhu počítače, vytížení procesoru a vytížení paměti.

U serveru je pak sledován opět status a doba běhu. Dále je sledována teplota vytížení procesoru spolu s vytížením paměti a využitím úložiště.

Router Info		
STATUS:	ON	15.12.2018 22:04
UPTIME:	47 days, 13:39:14.00	15.12.2018 22:04
OS VERSION:	6.42.7	15.12.2018 22:04
RAM LOAD:	26/65 MB (40%)	15.12.2018 22:04
HDD USAGE:	17/131 MB (13%)	15.12.2018 22:04
PC Info		
STATUS:	ON	15.12.2018 22:04
UPTIME:	3:47:27.39	15.12.2018 22:04
CPU LOAD:	35%	15.12.2018 22:04
RAM LOAD:	9/24 GB (38%)	15.12.2018 22:04
Server Info		
STATUS:	ON	15.12.2018 22:04
UPTIME:	up 2 hours, 3 minutes	15.12.2018 22:04
CPU TEMP:	35 °C	15.12.2018 22:04
CPU LOAD:	0.00	15.12.2018 22:04
RAM LOAD:	103/927MB (11.11%)	15.12.2018 22:04
HDD USAGE:	1/30GB (6%)	15.12.2018 22:04

This site is for proprietary use only. Unauthorized access is prohibited!

Obrázek 4: Monitorovací systém – Monitorovací panel

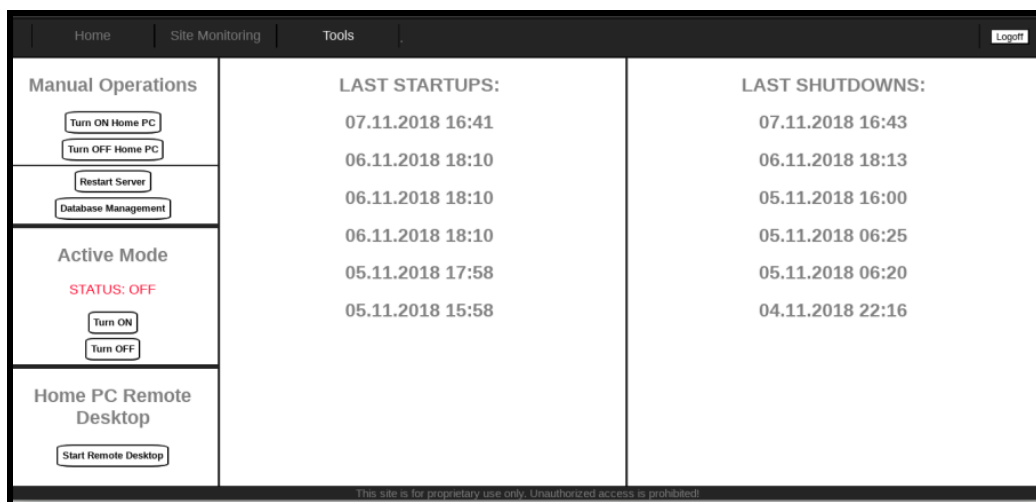
Jak jsem již zmiňoval výše v dokumentu, systém získává informace v intervalu pěti minut. Pokud ale se uživatel nachází v monitorovacím panelu, tak jsou informace získávány každou minutu. Důvodem pro snížení intervalu během prohlížení byla větší aktuálnost informací pro uživatele.

2.4.3 Ovládací panel

Skrze ovládací panel jsou dostupné všechny funkce vzdálené správy.

V ovládacím panelu jsou dostupné funkce vzdáleného vypnutí a zapnutí stolního počítače, restartování serveru, přístup do webového rozhraní databáze, aktivní režim a přístup ke vzdálené ploše stolního počítače. Dále se zde pak nachází výčet posledních šesti použití funkcí zapnutí a vypnutí stolního počítače.

Provádění příkazů a spouštění skriptů, které jsou potřebné k funkčnosti ovládacích funkcí panelu je prováděno pomocí PHP. Např. stisknutí tlačítka na zapnutí počítače spustí na stránce PHP skript, který serveru odešle příkaz k provedení startu počítače.



Obrázek 5: Monitorovací systém – Ovládací panel

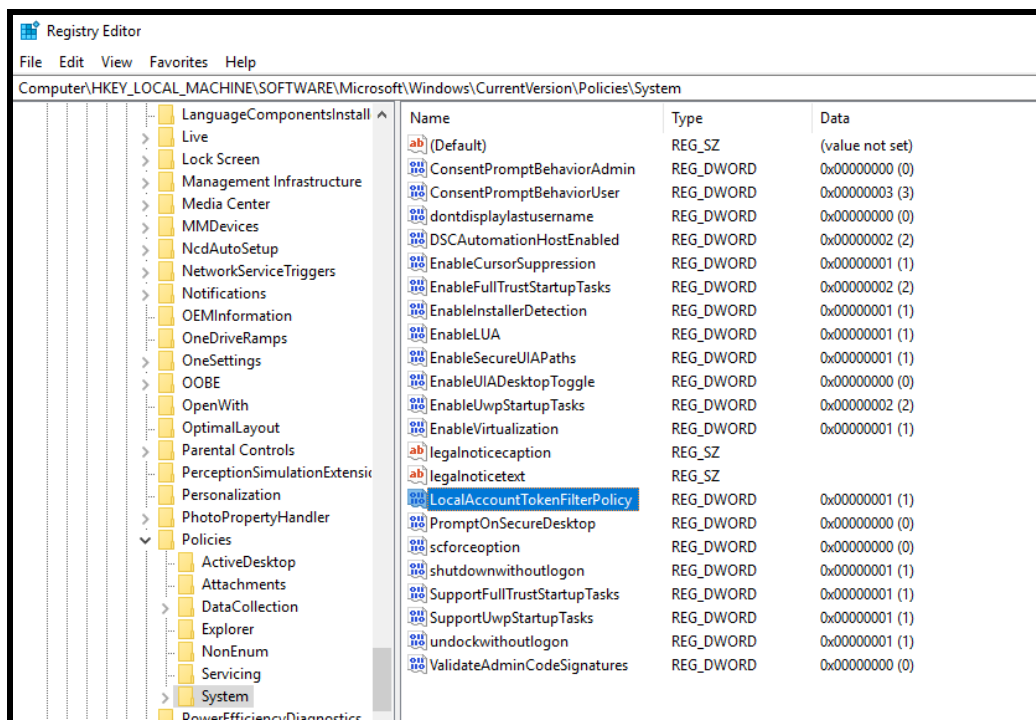
2.4.3.1 Vzdálené spuštění a vypínání PC

Ke vzdálenému spouštění využívám linuxový balíček etherwake. Po stisknutí tlačítka na stránce se provede PHP skript, který serveru odešle příkaz.

Příkaz vypadá takto: `sudo etherwake -i eth0 44:8A:5B:86:E0:CE`

Pro vzdálené vypnutí využívám skrytého administrativního sharu C\$, který umožňuje pomocí sdílení souborů administrátorský přístup k disku C, díky čemuž jsem schopen na dálku zadávat administrativní příkazy.

Abych ale mohl tento share používat, musel jsem do Windows 10 přidat registr LocalAccountTokenFilterPolicy, který obchází UAC zabezpečení pro sdílení souborů. Jde sice o bezpečnostní riziko, ale v uzavřené domácí síti nehraje až takovou roli.



Obrázek 6: Monitorovací systém – Přidaný registr

Kvůli využívání sdílení souborů s OS Windows jsem musel nainstalovat Sambu, která zajišťuje kompatibilitu při sdílení souborů mezi OS Windows a OS Linux.

Samotné vypnutí server provede tímto příkazem: `sudo net rpc shutdown -I 192.168.20.5 -U Jakub_Landa%admin`

Server se tímto ověří pod administrátorskými právy na stolním počítači a odešle mu příkaz k vypnutí. Počítač je následně vypnut.

Při každém použití funkce k vypnutí či zapnutí si stránka uloží čas a datum, kdy se funkce spustila a tato data uloží do databáze. Z těchto dat pak vzniká výpis, který je vidět na ovládacím panelu.

2.4.3.2 Aktivní režim

Aktivní režim je skript, která hlídá, jestli se uživatel nachází v domě či nikoliv. Pokud skript zjistí, že se uživatel nachází uvnitř domu, tak zapne stolní počítač a vypne se. Účelem skriptu je tedy zapnutí stolního počítače při příchodu uživatele z práce či školy a zpříjemnění uživatelského života.

Skript po zapnutí dvacet minut čeká. Dvacetiminutová prodleva je zvolena z toho důvodu, aby bylo umožněno uživateli odejít z domu.

Po uplynutí dvaceti minut začne skript každou minutu posílat ping na IP adresu uživatelského mobilního telefonu. Ověřování přítomnosti uživatele tedy probíhá pomocí pingu. Skript počítá s tím, že pokud dnes někam jdeme, tak máme mobilní telefon u sebe.

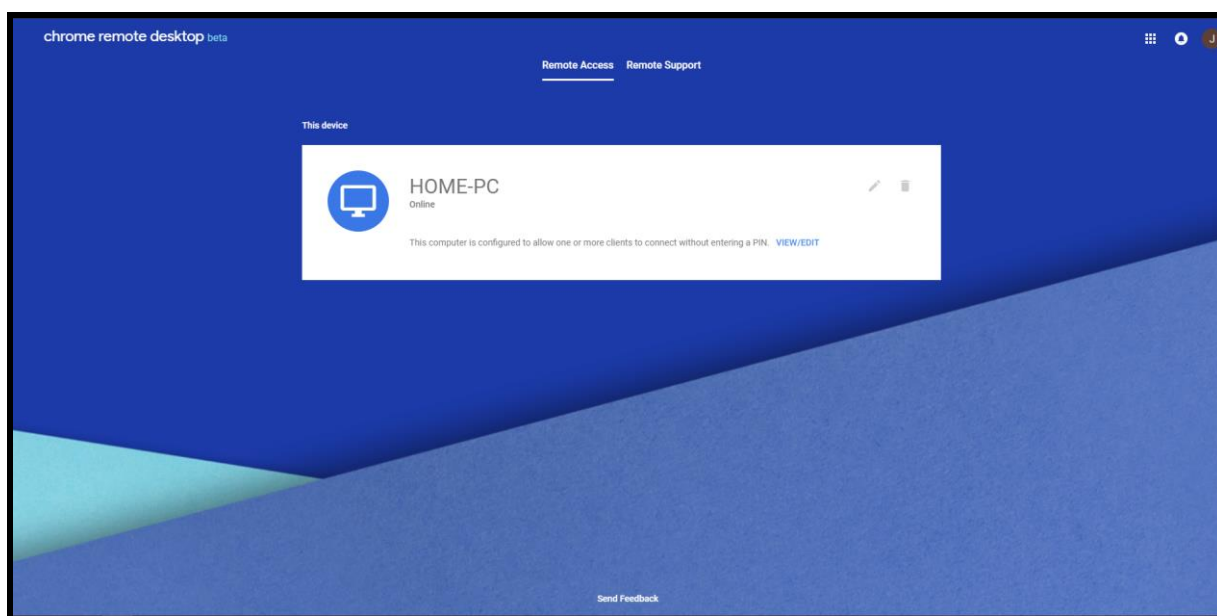
Jakmile skript dostane od mobilního telefonu odpověď, zapne stolní počítač. Skript se dá ukončit odpovědí mobilního telefonu nebo pomocí tlačítka k vypnutí aktivního režimu, které se nachází v ovládacím panelu.

2.4.3.3 Vzdálená plocha

Pro vzdálený přístup k počítači využívám vzdálenou plochu Chrome Remote Desktop beta.

Jedná se o převedení známého rozšíření pro prohlížeč Google Chrome do webové aplikace. Díky tomu stačí mít pouze nainstalovaného klienta vzdálené plochy na koncovém zařízení, na které se uživatel chce připojit. Velkou výhodou pro mě bylo, že jsem tuto webovou aplikaci mohl integrovat do mé práce a plně využít, jelikož je uživatelsky velmi přívětivá a nabízí vysokou kvalitu přenosu obrazu.

Protože jde o webovou aplikaci od společnosti Google, je nutné mít pro používání zřízený Účet Google a nainstalovaný prohlížeč Google Chrome. Osobně v tom ale nevidím nevýhodu.



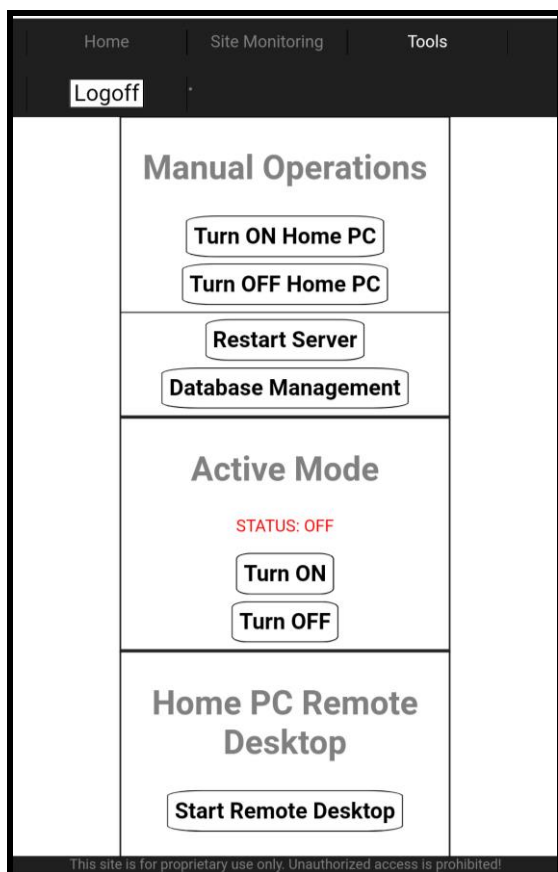
Obrázek 7: Monitorovací systém – Vzdálená plocha Chrome Remote Desktop beta

2.4.3.4 Mobilní verze ovládacího panelu

Jak jsem již zmiňoval, upravil jsem vzhled ovládacího panelu pro smartphone tak, aby bylo ovládání rychlé a snadné bez nutnosti přiblížování obrazovky.

Detekce mobilního zařízení probíhá na základě rozlišení obrazovky zařízení. Pokud je šířka menší než šest set pixelů, je automaticky načtena mobilní verze stránek.

Úpravu stránky jsem pojal ve stylu dálkového ovládacího panelu, kvůli čemuž jsem vynechal výpisy o posledních vypnutích a zapnutích.



Obrázek 8: Monitorovací systém – Mobilní verze ovládacího panelu

ZÁVĚR

Dokončením mého projektu monitorovacího systému jsem si utvrdil teoretické znalosti získané z výuky ve škole a praktické znalosti získané z praxe.

Získal jsem také mnoho nových znalostí v oboru informačních technologií. Nejvíce znalostí jsem získal z oblasti prostředí operačního systému Linux v rámci nastavování webového serveru a databáze. Hodně mi také přineslo vytváření stránek spolu s prací v databázi MariaDB.

S mou prací ale nekončím a plánuji ji rozvíjet i do budoucna, jelikož mám ještě mnoho nerealizovaných nápadů jako třeba vykreslování grafů, které by šlo do systému zakomponovat.

PŘÍLOHY

Příloha 1: Skript pro získávání a ukládání informací (dbscript.sh)

```
#!/bin/bash
```

```

#-----SERVER-----
-----

if ping -c 1 127.0.0.1 > /dev/null
then
    status="ON"
    date=$(date +%d.%m.%Y %H:%M')
    uptime=$(uptime -p)
    ramload=$(free -m | awk 'NR==2{printf "%s/%sMB (%.2f%%)\n",
$3,$2,$3*100/$2 }')
    freedisk=$(df -h | awk '$NF=="/{printf "%d/%dGB (%s)\n",
$3,$2,$5}')
    cpuload=$(top -bn1 | grep load | awk '{printf "%.2f\n", $(NF-
2)}')
    cput=$(cut -c1-2 < /sys/class/thermal/thermal_zone0/temp)
    cputemp=$(echo "$cput °C")

    mysql -u databaseadmin --password=SQLpasswd -e "USE
home_monitoring_database; INSERT INTO monitoringserver (ID, DATE,
STATUS, UPTIME, CPULOAD, CPUTEMP, RAMLOAD, HDDUSAGE) VALUES (NULL,
'$date', '$status', '$uptime', '$cpuload', '$cputemp', '$ramload',
'$freedisk');"

else
    status="OFF"
    date=$(date +%d.%m.%Y %H:%M')
    uptime="N/A"
    ramload="N/A"
    freedisk="N/A"
    cpuload="N/A"
    cput="N/A"
    cputemp="N/A"

    mysql -u databaseadmin --password=SQLpasswd -e "USE
home_monitoring_database; INSERT INTO monitoringserver (ID, DATE,
STATUS, UPTIME, CPULOAD, CPUTEMP, RAMLOAD, HDDUSAGE) VALUES (NULL,
'$date', '$status', '$uptime', '$cpuload', '$cputemp', '$ramload',
'$freedisk');"
fi

#-----ROUTER-----
-----

if ping -c 1 192.168.20.1 > /dev/null
then

    rstatus="ON"

    ruptime=$(snmpget -v2c -c secure -Ovn 192.168.20.1
.1.3.6.1.2.1.1.3.0 | cut -c 23-45)

    rosersion=$(snmpget -v2c -c secure -Ovn 192.168.20.1
1.3.6.1.4.1.14988.1.1.4.4.0 | cut -c 10-15)

    rmem1=$(snmpget -v2c -c secure -Ov 192.168.20.1
.1.3.6.1.2.1.25.2.3.1.5.65536 | cut -c 9-20)

```

```

    rmem2=$(snmpget -v2c -c secure -Ov 192.168.20.1
.1.3.6.1.2.1.25.2.3.1.6.65536 | cut -c 9-20)
    rmemsum=$((($rmem2 / ($rmem1 / 100)))
    rmemsum1=$((($rmem1 / 1000))
    rmemsum2=$((($rmem2 / 1000))

    rmemload=$(echo "$rmemsum2/$rmemsum1 MB ($rmemsum%)")

    rhdd1=$(snmpget -v2c -c secure -Ov 192.168.20.1
1.3.6.1.2.1.25.2.3.1.5.131072 | cut -c 9-20)
    rhdd2=$(snmpget -v2c -c secure -Ov 192.168.20.1
1.3.6.1.2.1.25.2.3.1.6.131072 | cut -c 9-20)
    rhddsum1=$((($rhdd1 / 1000))
    rhddsum2=$((($rhdd2 / 1000))
    rhddsum=$((($rhdd2 / ($rhdd1 / 100)))

    rhddspace=$(echo "$rhddsum2/$rhddsum1 MB ($rhddsum%)")

    mysql -u databaseadmin --password=SQLpasswd -e "USE
home_monitoring_database; INSERT INTO monitoringrouter (ID, DATE,
STATUS, UPTIME, OSVERSION, RAMLOAD, HDDUSAGE) VALUES (NULL, '$date',
'$rstatus', '$ruptime', '$rosversion', '$rmemload', '$rhddspace');"

else    rstatus="OFF"
        ruptime="N/A"
        rosversion="N/A"
        rmemload="N/A"
        rhddspace="N/A"

        mysql -u databaseadmin --password=SQLpasswd -e "USE
home_monitoring_database; INSERT INTO monitoringrouter (ID, DATE,
STATUS, UPTIME, OSVERSION, RAMLOAD, HDDUSAGE) VALUES (NULL, '$date',
'$rstatus', '$ruptime', '$rosversion', '$rmemload', '$rhddspace');"
fi

#-----PC-----
-----

if ping -c 1 192.168.20.5 > /dev/null
then

    pcstatus="ON"

    pcuptime=$(snmpwalk -v2c -c secure -Ovn 192.168.20.5
1.3.6.1.2.1.25.1.1 | cut -c 21-40)

    pccpu1=$(snmpget -v2c -c secure -Ovn 192.168.20.5
1.3.6.1.2.1.25.3.3.1.2.4 | cut -c 9-12)
    pccpu2=$(snmpget -v2c -c secure -Ovn 192.168.20.5
1.3.6.1.2.1.25.3.3.1.2.5 | cut -c 9-12)
    pccpu3=$(snmpget -v2c -c secure -Ovn 192.168.20.5
1.3.6.1.2.1.25.3.3.1.2.6 | cut -c 9-12)
    pccpu4=$(snmpget -v2c -c secure -Ovn 192.168.20.5
1.3.6.1.2.1.25.3.3.1.2.7 | cut -c 9-12)
    pccpu5=$(snmpget -v2c -c secure -Ovn 192.168.20.5
1.3.6.1.2.1.25.3.3.1.2.8 | cut -c 9-12)
    pccpu6=$(snmpget -v2c -c secure -Ovn 192.168.20.5
1.3.6.1.2.1.25.3.3.1.2.9 | cut -c 9-12)

```

```

        pccpu7=$(snmpget -v2c -c secure -Ovn 192.168.20.5
1.3.6.1.2.1.25.3.3.1.2.10 | cut -c 9-12)
        pccpu8=$(snmpget -v2c -c secure -Ovn 192.168.20.5
1.3.6.1.2.1.25.3.3.1.2.11 | cut -c 9-12)
        pccpusum=$((($pccpu1 + $pccpu2 + $pccpu3 + $pccpu4 + $pccpu5
+$pccpu6 + $pccpu7 + $pccpu8) / 8))

        pccpuload=$(echo "$pccpusum%")

        pcram1=$(snmpget -v2c -c secure -Ovn 192.168.20.5
1.3.6.1.2.1.25.2.3.1.6.2 | cut -c 10-20)
        pcram2=$(snmpget -v2c -c secure -Ovn 192.168.20.5
1.3.6.1.2.1.25.2.3.1.5.2 | cut -c 10-20)
        pcramsum1=$((($pcram1 / 10000000))
        pcramsum2=$((($pcram2 / 10000000))

        pcramsum=$((($pcram1 / ($pcram2 / 100)))
        pcramload=$(echo "$pcramsum1/$pcramsum2 GB ($pcramsum%)")

        mysql -u databaseadmin --password=SQLpasswd -e "USE
home_monitoring_database; INSERT INTO monitoringpc (ID, DATE, STATUS,
UPTIME, CPULOAD, RAMLOAD) VALUES (NULL, '$date', '$pcstatus',
'$pcuptime', '$pccpuload', '$pcramload');"

else    pcstatus="OFF"
        pcuptime="N/A"
        pccpuload="N/A"
        pcramload="N/A"

        mysql -u databaseadmin --password=SQLpasswd -e "USE
home_monitoring_database; INSERT INTO monitoringpc (ID, DATE, STATUS,
UPTIME, CPULOAD, RAMLOAD) VALUES (NULL, '$date', '$pcstatus',
'$pcuptime', '$pccpuload', '$pcramload');"

fi

```

Příloha 2: Skript pro aktivní režim (active.sh)

```

#!/bin/bash
mysql -u databaseadmin --password=SQLpasswd -e "USE
home_monitoring_database; REPLACE INTO active (ACTIVE) VALUES ("1");"
sleep 20m
while [ 0 -lt 1 ]
do

    if ping -c 1 192.168.20.3 > /dev/null 2>&1;
    then
        starttime=$(date '+%d.%m.%Y %H:%M')
        mysql -u databaseadmin --password=SQLpasswd -e "USE
home_monitoring_database; INSERT INTO startuplog (ID, DATE) VALUES
(NULL, '$starttime');"
        mysql -u databaseadmin --password=SQLpasswd -e "USE
home_monitoring_database; REPLACE INTO active (ACTIVE) VALUES ("0");"
        etherwake -i eth0 44:8A:5B:86:E0:CE
        exit 0
    fi

```

done

Seznam použitých obrázků

Obrázek 1: Monitorovací systém – Server.....	12
Obrázek 2: Monitorovací systém – Přihlašovací stránka.....	14
Obrázek 3: Monitorovací systém – Domovská stránka	15
Obrázek 4: Monitorovací systém – Monitorovací panel.....	16
Obrázek 5: Monitorovací systém – Ovládací panel.....	17
Obrázek 6: Monitorovací systém – Přidaný registr	18
Obrázek 7: Monitorovací systém – Vzdálená plocha Chrome Remote Desktop beta.....	19
Obrázek 8: Monitorovací systém – Mobilní verze ovládacího panelu	20

Použité zkratky

BIOS – Basic Input Output Systém; UEFI - Unified Extensible Firmware Interface; OS – operační systém; OID – Object Identifier; MAC – Media Access Control ; UDP – User Datagram Protocol; SNMP – Simple Network Management Protocol; MIB – Management Information Base; IP – Internet Protocol

POUŽITÉ INFORMAČNÍ ZDROJE

RFC 1157 - A Simple Network Management Protocol (SNMP) [online]. Fremont, Kalifornie, USA: Internet Engineering Task Force [cit. 2018-12-16]. Dostupné z:

<https://tools.ietf.org/html/rfc1157>

RFC 1066 - Management Information Base for Network Management of TCP/IP-based internets [online]. Fremont, Kalifornie, USA: Internet Engineering Task Force, 1988 [cit. 2018-12-16]. Dostupné z: <https://tools.ietf.org/html/rfc1066>

SNMP - Simple Network Management Protocol < články -> SAMURAJ-cz.com [online]. Hluboká nad Vltavou: Petr Bouška, 2006 [cit. 2018-12-16]. Dostupné z:

<https://www.samuraj-cz.com/clanek/snmp-simple-network-management-protocol/>

SNMP - Simple Network Management Protocol - Wikipedia [online]. San Francisco: Wikimedia Foundation, 2018 [cit. 2018-12-16]. Dostupné z:

https://en.wikipedia.org/wiki/Simple_Network_Management_Protocol

Wake-on-LAN - Wikipedia [online]. San Francisco: Wikimedia Foundation, 2018 [cit. 2018-12-16]. Dostupné z: <https://en.wikipedia.org/wiki/Wake-on-LAN>

Administrative share - Wikipedia [online]. San Francisco: Wikimedia Foundation, 2018 [cit. 2018-12-16]. Dostupné z: https://en.wikipedia.org/wiki/Administrative_share