CUSTOMER MONITOR

Monitoring prenosených dát cez internet

verzia ku dňu 18.11.2009 a k verzii C-Monitoru 2.0.1.468

SEAL

SEAL IT Services, s.r.o.

Kontakt: **SEAL IT Services, s.r.o.**, Topoľová 4, 811 04 Bratislava 1, tel.: +421 2 5465 0242, fax: 02/5478 9664 podpora: support@customermonitor.net, web: **www.customermonitor.sk**

Obsah

1 Úvod

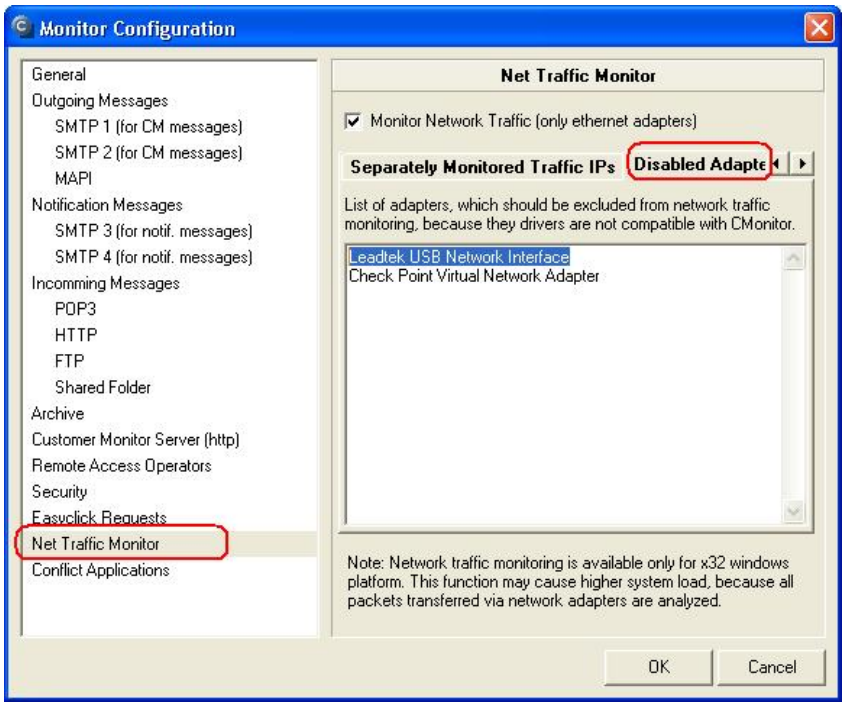
1.1 Úloha Monitoringu prenesených dát cez internet v CM

Monitorovanie prenosu dát cez internet má dôležitý význam pri správe IT. Internet dnes predstavuje ako aj úžitok tak i hrozbu, ktorú je potrebné mať pod kontrolou. Monitoring internetových prenosov v Customer Monitore nezasahuje do súkromia používateľa - nezbiera informácie o navštívených webstránkach. Dôraz je v odhalení hraničných stavov, ovplyvňujúcich ostatných používateľov ako je preťaženie linky s jednoduchým určením akým procesom a na akú lokalitu sú dáta prenášané. Taktiež je cieľom pomôcť určiť prejav škodlivých kódov (trójskych koní).

1.2 Upozornenie k možnosti blokácie sieťovej komunikácie

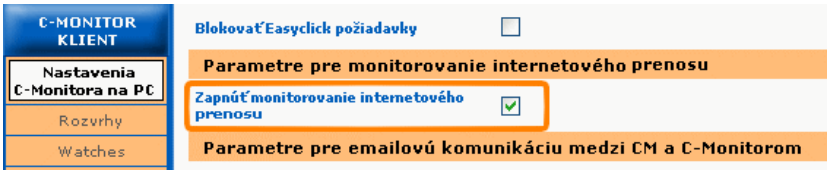
Ak je na počítači zapnutý monitoring internetových prenosov, vo výnimočných prípadoch môže prísť k blokácii sieťovej komunikácie cez sledované adaptéry. Prejavuje sa to nefunkčnou sieťovou komunikáciou pár minút od naštartovania počítača, pričom signalizácia pripojenia neindikuje žiaden problém. Tento problém sa objavuje iba pri špecifických typoch sieťových adaptérov (niektoré USB modemy, VPN adaptéry napr. Checkpoint)

Ak daný problém zistíte, je možné konkrétny sieťový adaptér vylúčiť z monitoringu v konfigurácii C-Monitora. Predvolene sú do monitoringu zahrnuté automaticky všetky nájdené adaptéry. Prejdite do časti *Net Trafic monitor*, nalistujte záložku Disabled adapters a pripíšte do konfigurácie blokovaný sieťový adaptér.



Obrázok č 1 Vylúčenie sieťového adaptéra zo sieťového monitoringu (internetových prenosov).

Taktiež existuje možnosť vypnúť monitoring internetových prenosov na danom počítači úplne. Zvážte túto možnosť až ako poslednú, nakoľko tento monitoring dokáže odhaliť zavírenie, zneužitie počítača určitými programami alebo poruchu softvéru, ktorý zahltí internetové spojenie. Môžete to spraviť cez Server CM. *Admin.zóna -> C-Monitor klient -> Nastavenia C-Monitora na PC* a v danom počítači vypnite možnosť *Zapnúť monitorovanie internetových prenosov*.



Obrázok č.2 Vypnutie sieťového monitoringu (internetových prenosov) na zvolenom počítači cez Server CM.

2 Základný prehľad

2.1 Princíp funkčnosti

Údaje o prenesených dátach sú zbierané na počítačoch s inštalovaným C-Monitor klientom od verzie **2.0.1.448**. Prostredníctvom HTTP protokolu sú doručované do Servera CM. Na Serveri CM je automatizovane zistené na základe MAC adresy a IP adresy z predvolenej brány, do akej siete počítač patrí a taktiež sú umožnené štatistiky za celú sieť. Ideálne je teda, aby všetky počítače mali nainštalovaný C-Monitor.

Informácie o prenesených dátach cez internet v CM obsahujú

a) **aplikáciu/proces, ktorá dáta preniesla** (pokiaľ spojenie vzniklo po naštartovaní CMonitor klienta)
b) **port TCP / protokol UDP** cez ktorý dáta boli prenesené
c) **cieľovú IP adresu** - týka sa štatistík nad 1 hod

Obsahom údajov nie je web adresa z prehliadača.

2.2 Podporované operačné systémy, obmedzenia

2.2.1 Podporované OS

Windows 2000 a vyššie, vo verzii 32bit. 64bit. systémy budú podporené neskôr.

2.2.2 Známe obmedzenia a konflikty

Najvážnejším zaregistrovaným prípadom je nepríjemné obmedzenie sieťovej komunikácie na niektorých sieťových adaptéroch. Nepríjemnosť spočíva vo fungovaní sieťovej komunikácie krátko po štarte a za pár minút sa preruší. Takéto konfliktné sieťové adaptéry je možné vylúčiť z monitoringu a viac sa dočítate v bode *1.2 Upozornenie k možnosti blokácie sieťovej komunikácie.*

Ďalším známym obmedzením je konflikt s Integrovaným Firewallom v produkte ESET Smart Security (pre obidve súčasné verzie 3.0 aj 4.0), kedy sa počítač reštartoval ihneď po nabootovaní. CM Internet monitoring je možný pri tomto produkte len, ak úplne vypnete Integrovaný Personal Firewall. Vypnutie je realizovateľné v ESS 4.0 v Rozšírených nastaveniach na vetve : „Personal Firewall / System Integration“ - prepnúť do možnosti „Personal Firewall is completely disabled“. Ak tento firewall vypnete, doporučujeme aktivovať vstavaný Windows Firewall.

Ochrana proti konfliktnému produktu je automatizovaná a funguje tak, že ak sa nájde konfliktný produkt (Firewall v ESS), CMonitor sám vypne Internet monitoring.

CM Internet Monitoring je bez akýchkoľvek prestavení funkčný s NOD32 Antivirus (akákoľvek verzia). Nenašli sa ani problémy pri AVG 8.5, McAfee, CA eTrust antivír.

2.2.3 Doporučovaný prehliadač - Mozilla Firefox

Prístup na CM server je už pre vás známy a je prístupný prostredníctvom internetového prehliadača. Zvolená hlavná technológia pre ovládanie časti Internet Bandwith Monitoring a tiež pre SW audit, HW evidencia je Ajax. Výkon tejto časti je optimalizovaný

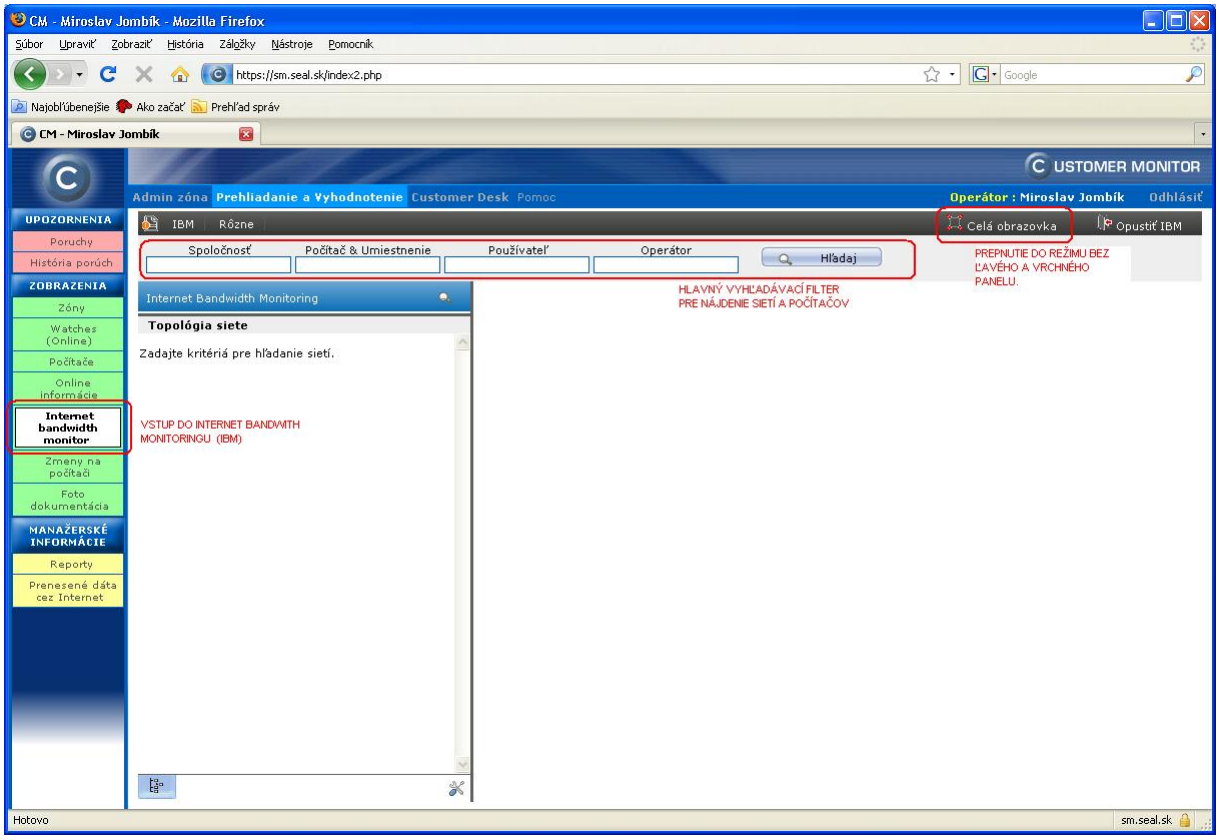
pre prehliadač Firefox Mozilla, oproti Internet Exploreru je rýchlosť citeľne vyššia. V ostatných prehliadačoch nie je garantovaný bezchybný chod.

3 Doporučovaná organizácia zariadení v IBM

3.1 Vstup do Internet Bandwith monitoringu (skratka IBM)

Všetky údaje o internetových prenosoch zozbierané z CMonitor klientov sa nachádzajú pod tlačidlom Internet Bandwith monitoringu v ľavom paneli. Následne sa vám objaví filter k vyhľadaniu počítačov. Počítače sa zobrazia v topológii detekovaných sietí, ktorých popis je nižšie.

Doporučujeme pre zväčšenie pracovnej plochy si kliknúť na odkaz v pravo hore „Celá obrazovka“. Pre vrátenie sa do zobrazenia v rámoch, stlačte odkaz „Okno“

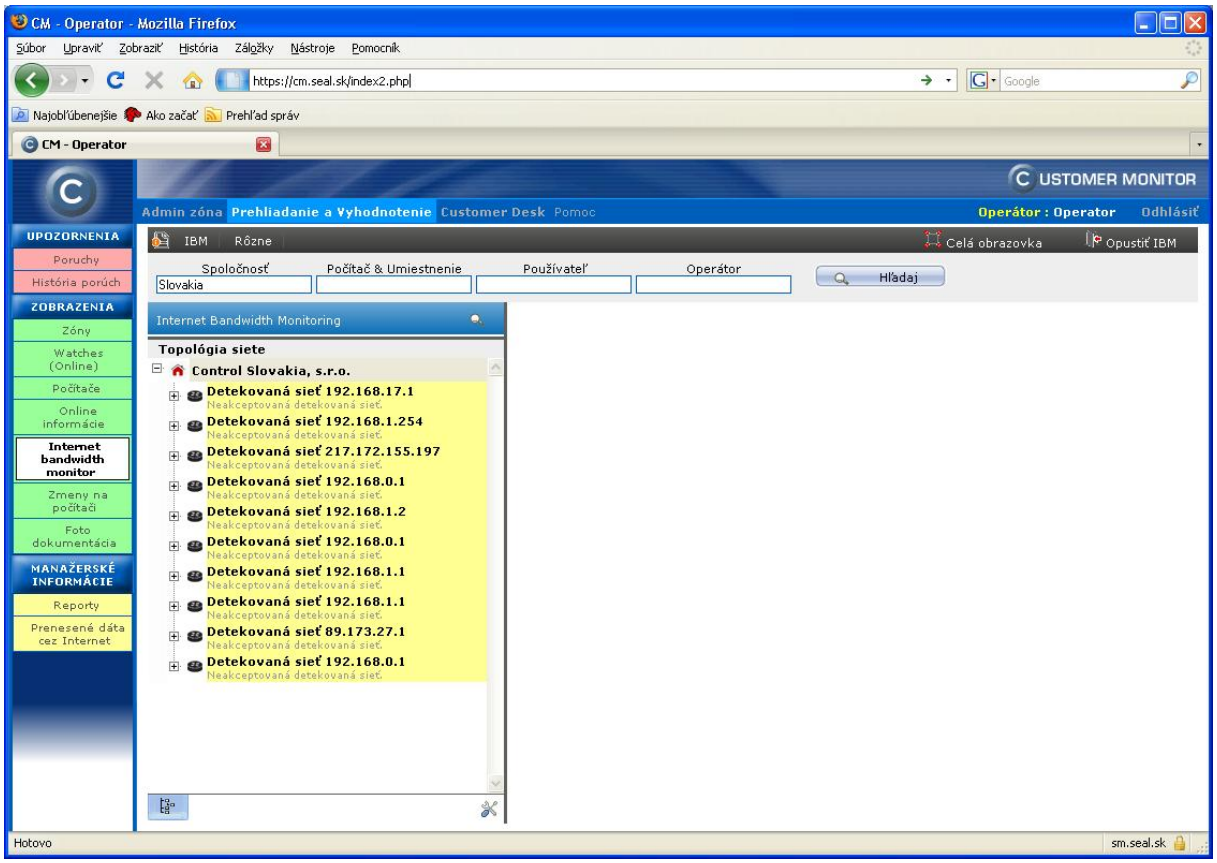


Obrázok č. 3 Vstup do Internet Bandwith Monitoring - monitorovania prenesených údajov cez internet

3.2 Automatická detekcia sietí

Aby bolo možné vyhodnotiť zaťaženie siete pri prenose cez internet, je potrebné, aby sa počítače zoskupili do topológie siete, ktorá zodpovedá reálnej sieti. Každý C-Monitor klient, ktorý komunikuje so Serverom CM posiela údaje o predvolenej bráne (MAC adresa, IP adresa). Na základe toho sa darí automatizovane určiť spojenie počítačov do jednej siete.

V Internet Bandwith Monitoringu po zadaní aspoň názvu spoločnosti máte vidieť v strome siete s názvom „Detekovaná sieť - IP predvolenej brány“ a po rozbalení sa objavia aktuálne alebo naposledy zapojené počítače v tejto sieti.



Obrázok č. 4 Automaticky detekované siete v Internet Bandwith Monitoringu (IBM)

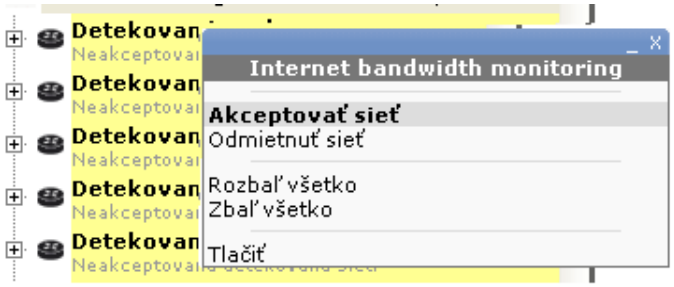
3.3 Akceptácia / Odmietnutie siete

Pre vytvorenie poriadku a sprístupnenia všetkých možností, ktoré Internet Bandwith Monitoring ponúka je potrebné sieť Akceptovať. Akceptáciu vykonajte len pre siete, s ktorými chcete ďalej pracovať (ich prostredie evidovať), inak v rámci postupu Akceptácie zvolíte „Odmietnuť“ alebo je možné ponechať sieť aj v nezmenenom stave - Detekovaná sieť.

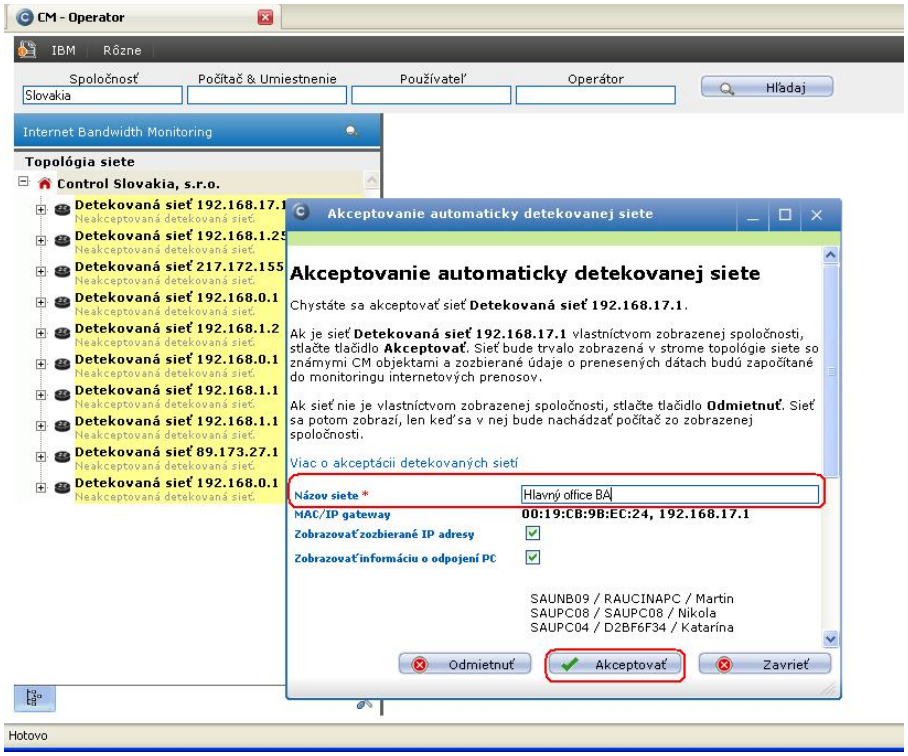
Akceptáciu doporučujeme , aby ste si mohli pomenovať sieť, kde sa nachádza a aké má použitie.

Stav „Odmietnutá“ sieť bude znamenať, že sa daná sieť stratí zo zoznamu sietí a objaví sa len pre momenty, keď je do tejto siete zapojený počítač s CMonitor klientom. Počítač sa zobrazí v Odmietnutej sieti, len keď patrí pod rovnakého správcu. V rámci možností zobrazenia k stromu topológie siete môžete odmietnuté siete vypnúť úplne.

Akceptáciu/Odmietnutie vykonáte stlačením pravého tlačidla myši nad zvolenou Detekovanou sieťou (tj. najprv kliknite na danú sieť a potom stlačte pravé tlačidlo myši). V ďalšom dialógu pomenujete sieť podľa vašich štandardov a upravte voľby ako si prajete strom siete zobraziť.

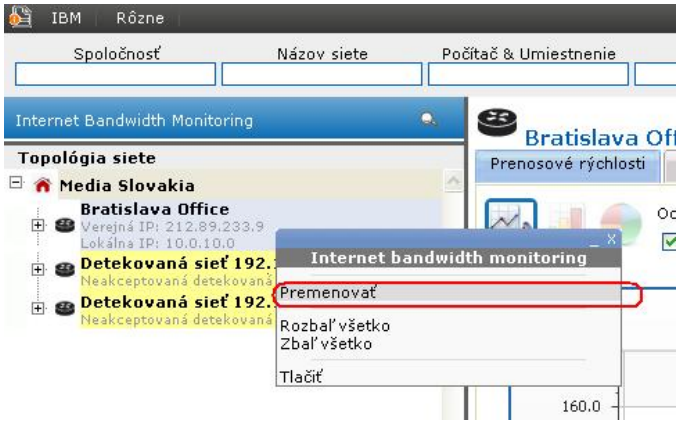


Obrázok č. 5 Akceptácia detekovanej siete v Internet Bandwith Monitoringu (IBM)



Obrázok č. 6 Akceptácia detekovanej siete- úprava názvu siete a následné stlačenie „Akceptovať“ premenovanie akceptovanej siete

Premenovanie už akceptovanej siete v Internet Bandwith Monitoringu (IBM) urobíte z kontextového menu k zvolenej sieti položkou „Premenovať“.

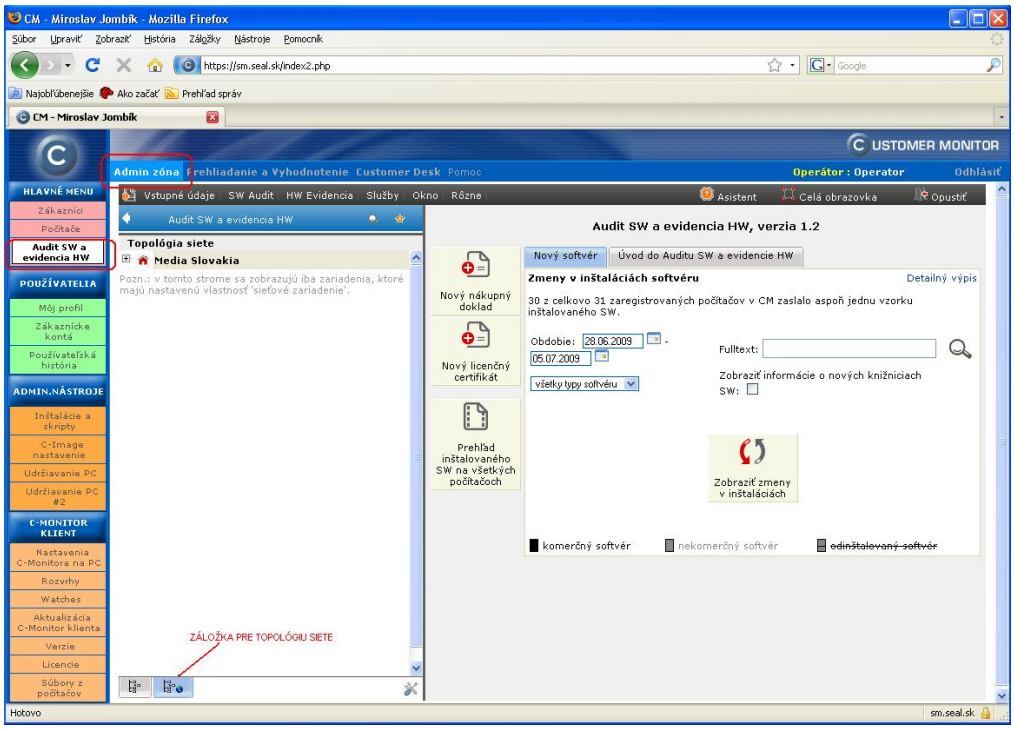


Obrázok č. 7 Premenovanie akceptovanej siete

3.4 Vytvorenie sieťovej vetvy, vloženie sieťového prvku (v SW a HW evidencii)

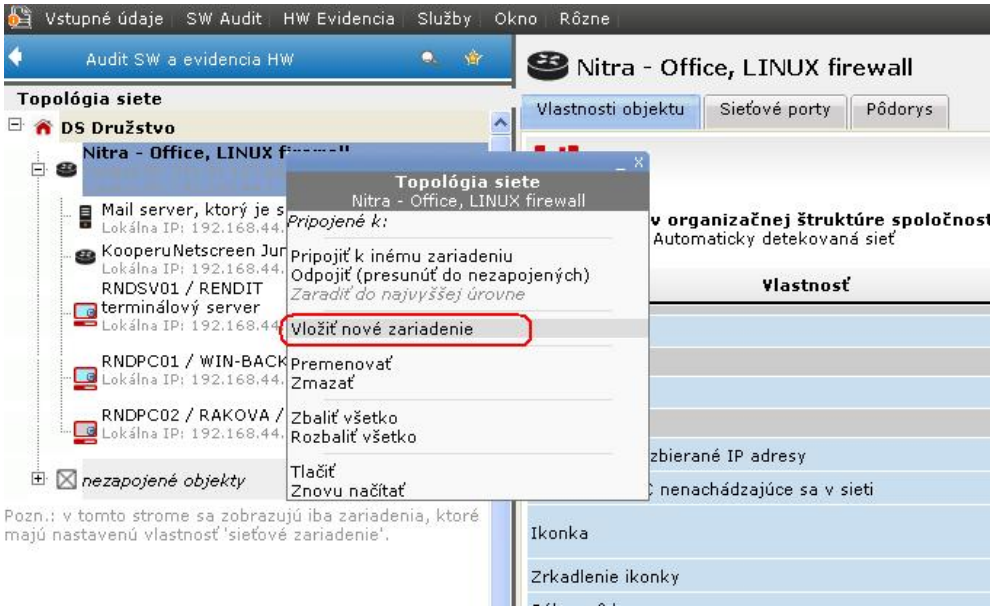
Strom sietí zobrazený v Internet Bandwith Monitoringu je totožný s Topológiou siete v časti SW audit, HW evidencia. Do stromu siete si môžete manuálne vložiť ďalšie sieťové prvky a popresúvať zapojenie počítačov, tak ako sú v skutočnosti zapojené. Získate tým nadhľad nad danou sieťou a v prípade poruchy sieťovej komunikácie sa vám bude jednoduchšie hľadať riešenie.

Úpravu stromu detekovanej siete je možné robiť len v časti SW audit, HW evidencia. (Admin.zóna -> Audit SW, HW evidencia -> výber spoločnosti -> prepnutie sa do záložky Topológia siete na spodu zobrazeného stromu)



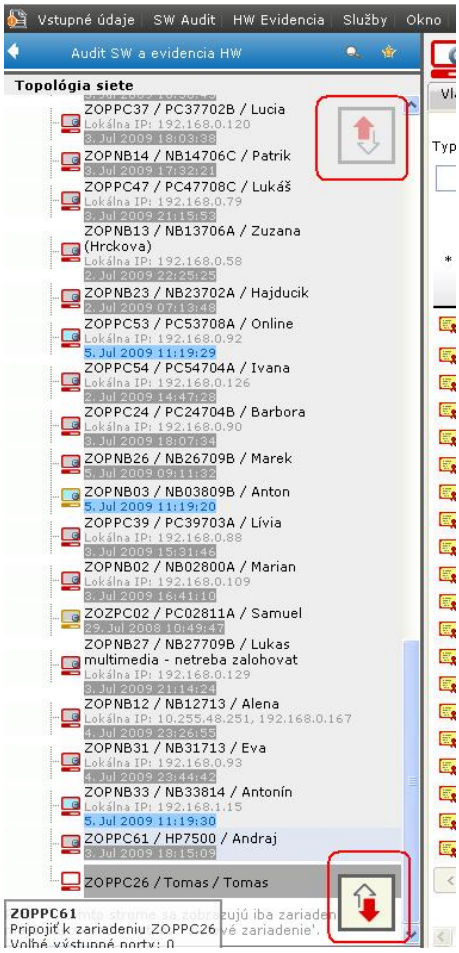
Obrázok č. 8 Vstup do topológie siete v rámci SW auditu, HW evidencie

Vložením vetviaceho sieťového prvku ako napríklad switch, router vytvoríte ďalšiu vetvu a do nej môžete vkladať koncové sieťové zariadenia (počítače, tlačiarne a podobne). Vloženie prvku uskutočníte z kontextového menu siete alebo už existujúceho sieťového prvku zvolením položky .



Obrázok č. 9 Vloženie nového prvku do topológie siete.

Premiestňovanie prvkov je jednoduchým spôsobom Drag&Drop. V prípade, že potrebujete premiestniť prvok do časti stromu, ktorá nie je viditeľná, zobrazia sa vám pomocné šípky, nad ktoré keď nadídete, strom sa posunie.

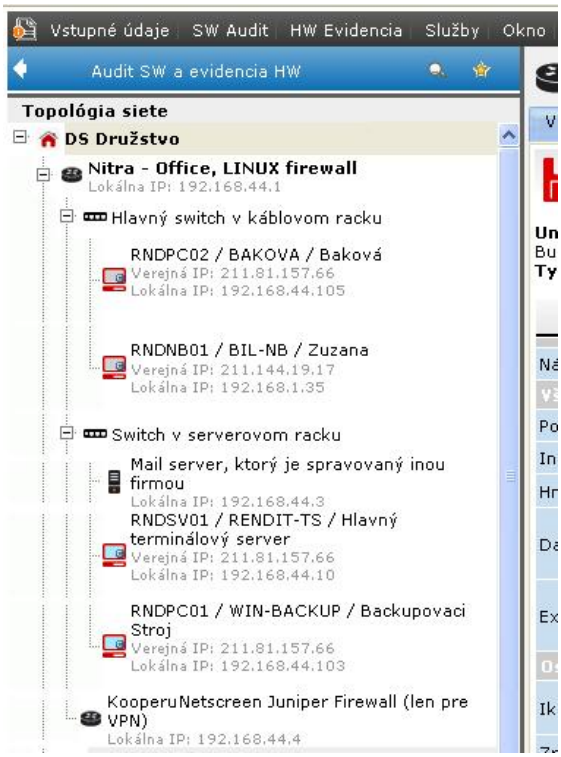


Obrázok č. 10 Pomocné posúvacie šípky pri presune zariadenia do nezobrazenej časti stromu siete.

Po zvolení cieľového prvku (vetvy siete) vás program vyzve pre zvolenie čísla portov, ktoré chcete prepojiť. Má to význam, ak si evidujete presné porty jednotlivých prepojení alebo pri zariadeniach, ktorých každý port má svoj vlastný význam. Názvy portov môžete zmeniť vo vlastnostiach daného zariadenia. Ak vám nezáleží na presnom priradení portov, stlačte tlačidlo Prepojiť vybrané porty.

Môže sa vám ešte stať, že sa pripájate na zariadenie, ktoré v evidencii nemá voľný port. Vtedy dostanete dialóg k vytvoreniu nového portu, buď si ho sami vytvoríte alebo si ho dáte vytvoriť automaticky.

Obrázok č. 11 Prepojenie portov po presune zariadenia.



Obrázok č. 12 Ukážka evidovanej topológie siete v CM zodpovedajúcej fyzickému zapojeniu.

4 Zobrazenie údajov o internetových prenosoch na Serveri CM

Informácie o prenesených údajoch cez internet z počítačov s nainštalovaným CMonitor klientom sú v CM v „*Prehliadanie a Vyhodnotenie -> Zobrazenia -> Internet Bandwith Monitoring*“. Pre viac informácií viď. *3.1 Vstup do Internet Bandwith monitoringu (skratka IBM)*.

Základný rámec poskytovaných informácií v Serveri CM je :

a) **Prenosová rýchlosť** za vybraný počítač alebo celú sieť / vybranú vetvu siete
b) **Objem prenesených dát** za vybraný počítač alebo za celú sieť / vybranú vetvu siete.

Druhy informácií ako už bolo uvedené vyššie v *2.1 Princíp funkčnosti* sú :

a) **aplikáciu/proces, ktorá dáta preniesla** (pokiaľ spojenie vzniklo po naštartovaní CMonitor klienta)
b) **port TCP / protokol UDP** cez ktorý dáta boli prenesené
c) **cieľovú IP adresu** (týka sa len štatistík v intervale nad 1 hod)

Obsahom údajov nie je web adresa z prehliadača.

Poznámka: Informácie o prenesených údajoch sú zatiaľ dostupné len z 32-bitových systémov a s vybranými obmedzeniami, napríklad musí byť vypnutý Personal Firewall v Eset Smart Security 4.0, pokiaľ ho používate.

4.1 Prehľad prenosov na internet za celú sieť / vetvu v topológii siete

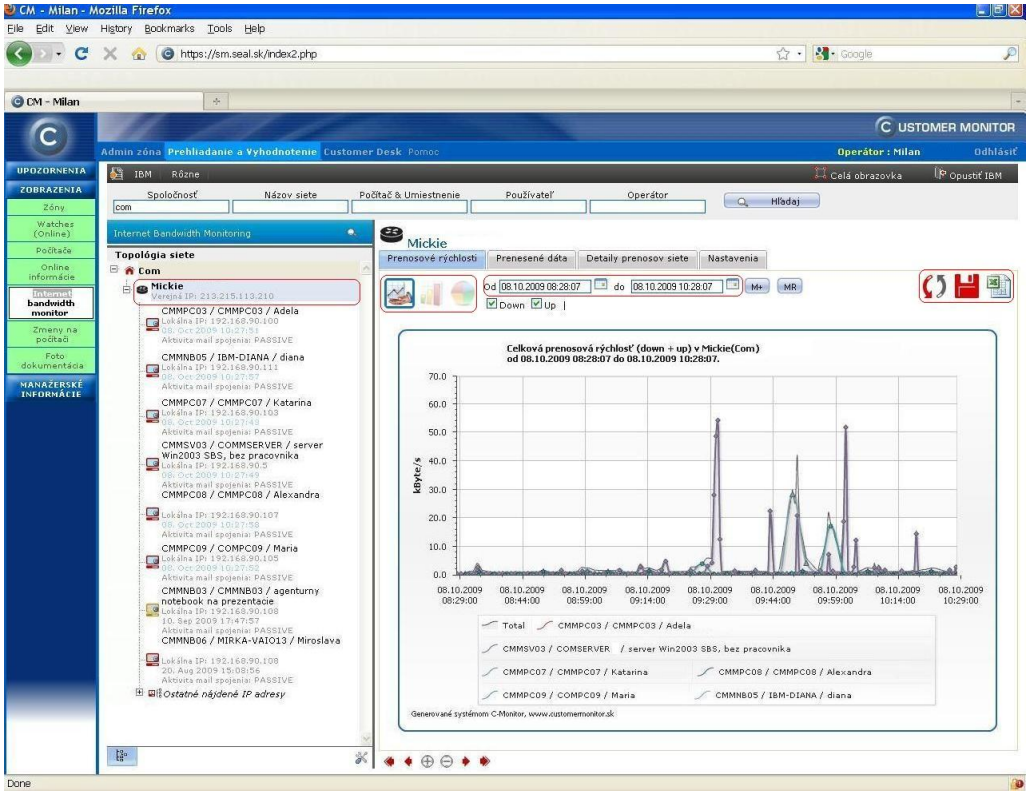
IBM ponúka podrobný prehľad prenosových rýchlostí ako aj prenesené dáta za danú sieť, ale aj za jednotlivé počítače. Začneme kliknutím na detekovanú sieť (nemusí byť akceptovaná) v topológii siete.

4.1.1 Prenosové rýchlosti a ich vykreslenie za celú sieť

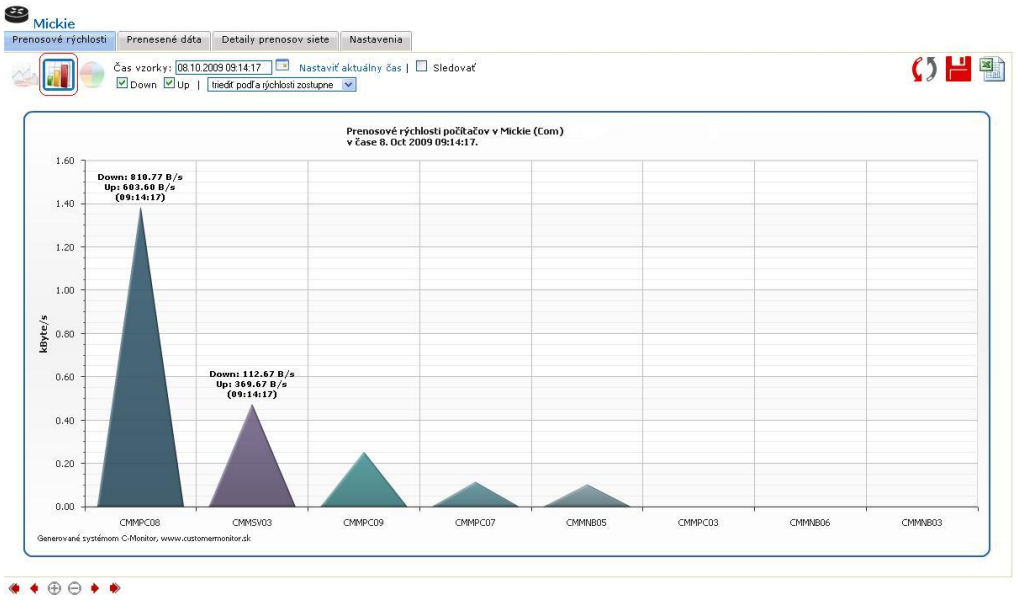
V pravej časti obrazovky sa automaticky vykreslia priebehy prenosových rýchlostí za posledné dve hodiny, štandardne download a upload za všetky počítače nachádzajúce sa v danej sieti. Každý počítač ma pridelenú vlastnú farbu v grafe. Podľa potreby sa dá zmeniť časový interval zobrazenia rýchlostí v hornej časti obrazovky priamym zvolením si požadovaného dátumu alebo v dolnej časti kliknutím na šípky  . Po zmene časového intervalu treba prekresliť graf nanovo stlačením tlačidla *Prekresliť graf*  v pravej horne časti.

Po kliknutí na ľubovoľnú bodku v grafe alebo vybraním zobrazenia *Stĺpcový graf* sa zobrazí prehľadný stĺpcový graf, ktorý popisuje prenosové rýchlosti jednotlivých počítačov, za sledované časové obdobie. Pre percentuálne zobrazenie prenosových rýchlostí jednotlivých počítačov v danej sieti zvolíme zobrazenie *Koláčový graf*. Zobrazené priebehy sa dajú

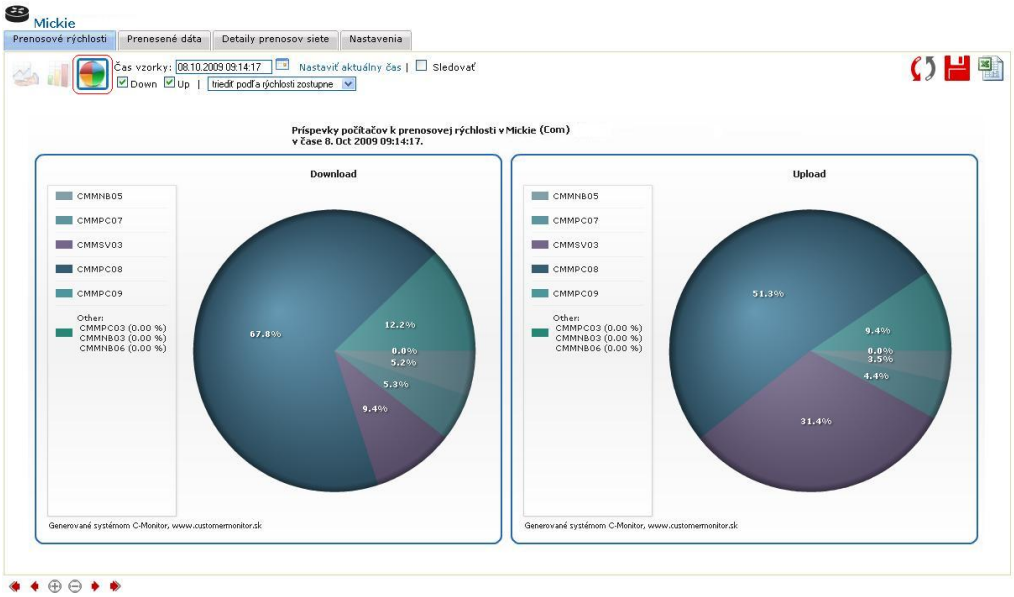
vyexportovať kliknutím na ikony  v pravej hornej časti do .png alebo do známeho excelovského .xls formátu.



Obrázok č. 13 Prenosové rýchlosti sa celú sieť, časový graf za posledné dve hodiny



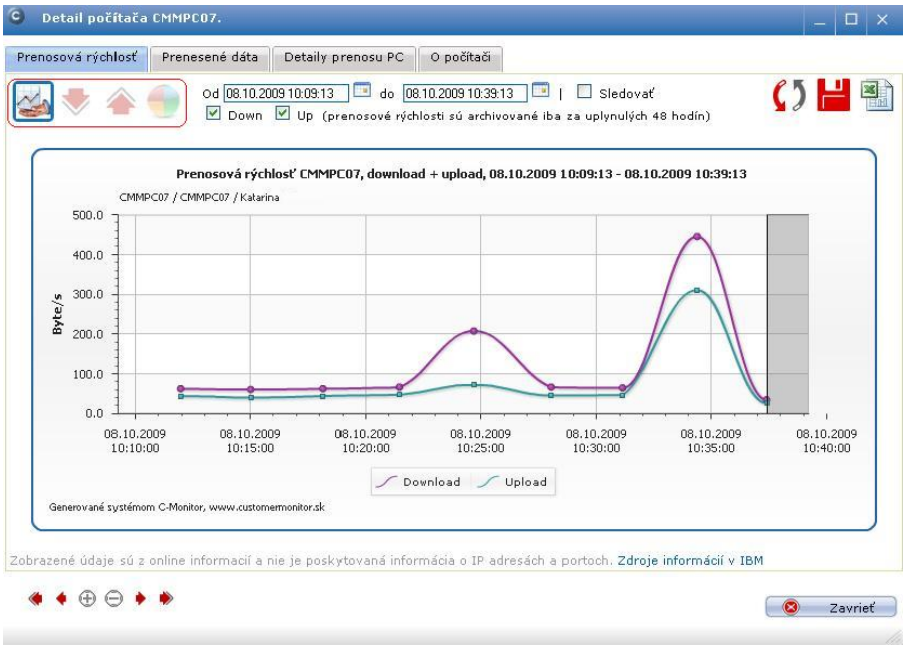
Obrázok č. 14 Prenosové rýchlosti počítačov, stĺpcový graf



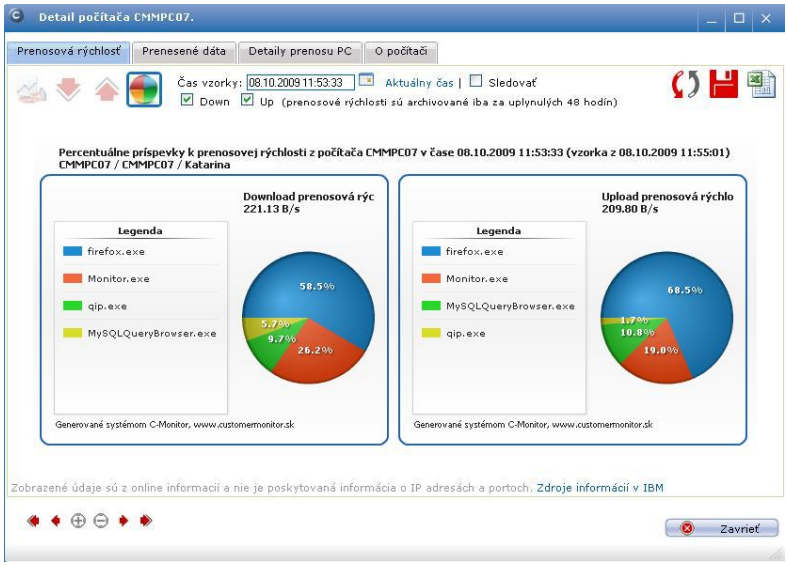
Obrázok č. 15 Percentuálne zobrazenie prenosových rýchlostí za celú sieť

4.1.2 Prenosové rýchlosti za konkrétny počítač

Prenosové rýchlosti za konkrétny počítač sa zobrazia v samostatnom okne po kliknutí na vybraný PC z topológie siete. Podľa požadovaného zobrazenia zvolíme v hornom menu kliknutím na ikony  zobrazenie celkovej *Prenosovej rýchlosti, Download procesov, Upload procesov* alebo *príspevky procesov.* Zmena časového intervalu je totožná ako pri pre prenosových rýchlostiach za celú sieť (4.1.1 Prenosové rýchlosti a ich vykreslenie za celú sieť). Pri zaškrtnutí *„Sledovať"* sa začne sledovaný priebeh automaticky aktualizovať.



Obrázok č. 16 Celková prenosová rýchlosť konkrétneho PC



Obrázok č. 17 Percentuálne rozdelenie rýchlostí jednotlivými aplikáciami

4.2 Kumulované prenesené dáta z počítačov v sieti

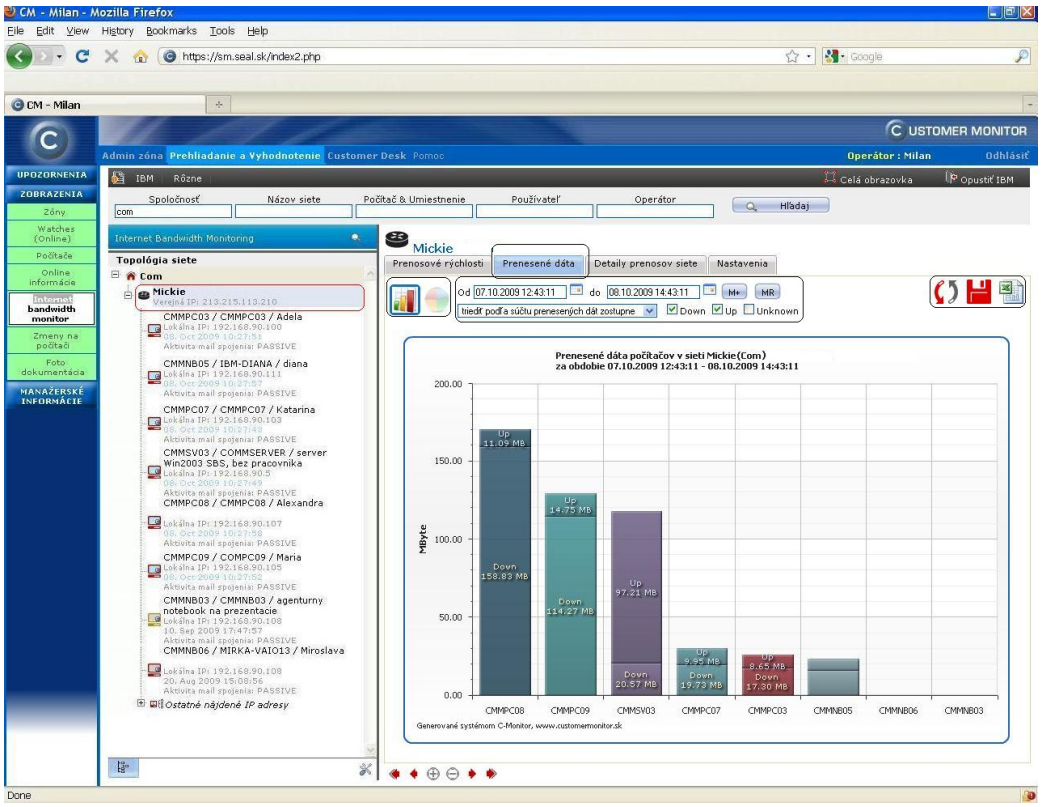
IBM ponúka detailnú možnosť výpisov o prenesených dátach za jednotlivý počítač i za celú spoločnosť. Na výber sú grafické a textové zobrazenia s podrobným popisom prenosov dát jednotlivých procesov cez porty a prenosy z IP adries.

4.2.1 Prenesené dáta za celú sieť

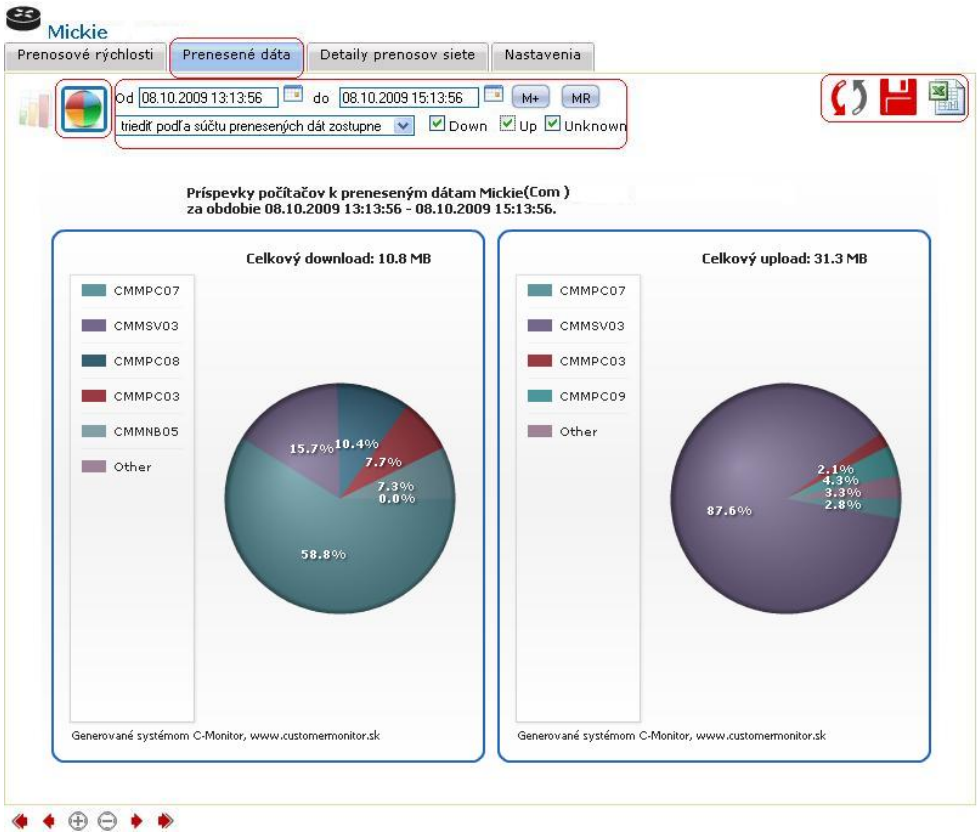
Prehľad o prenesených dátach za celú sieť získame obdobne ako v pri zobrazení prenosových rýchlostí kliknutím na detekovanú sieť v topológii siete a zvolíme v ľavej časti obrazovky záložku *Prenesené dáta*. Predvolene sa zobrazí stĺpcový graf s počítačmi zvolenej siete, kde je aj zobrazený objem prenesených dát za posledné dve hodiny. Zmenu časového intervalu, vypnutie alebo zapnutie zobrazenia *Downloadu, Uploadu, Unknown* ako aj kritérium pre zobrazenie grafu sa nastaví v hornej časti okna. Zobrazené grafy sa vyexportujú stlačením ikoniek do .png alebo .xls formátu.

Unknown je nerozpoznateľný prenos, ktorý vzniká, ak žiadosť o prenos príde z vonku. Ako príklad z inej siete bol prístup na disk a kopírovali sa údaje. Tiež sú tam zahrnuté prenosy maskovaných procesov.

V reálnom čase nie je možné poslať všetky údaje o prenose. Vieme zistiť celkový prenos. Rozdiel medzi celkovým prenosom a prenosom v reálnom čase je korekcia. Korekcia sa minimalizuje po získaní reportov, ktoré chodia v oneskorení niekoľko hodín.

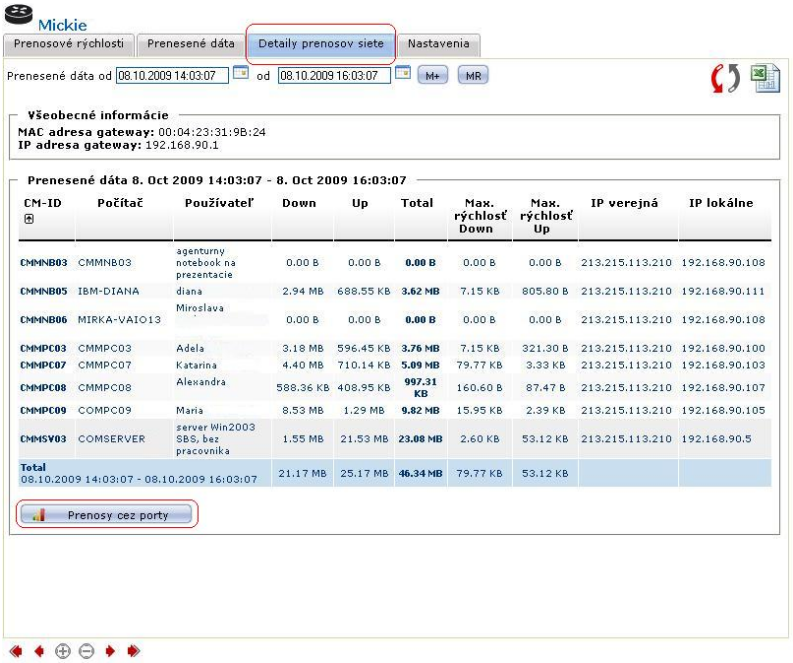


Obrázok č. 18 Prenesené dáta za celú sieť s detailom na jednotlivé PC vo vybranej sieti

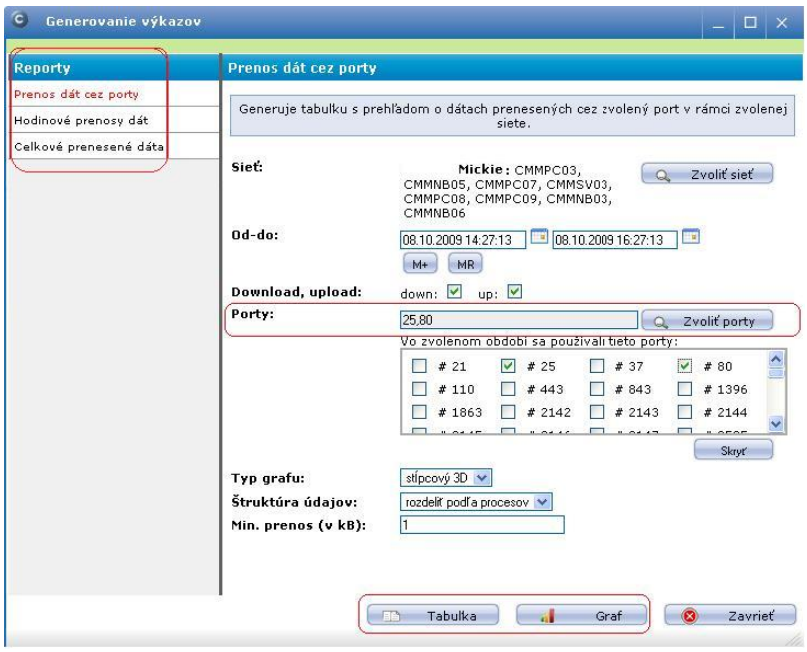


Obrázok č. 19 Prenesené dáta za celú sieť percentuálny podiel počítačov, koláčový graf

V záložke *Detaily prenosov siete* je detailný prehľad jednotlivých počítačov a ich aktivite za zvolený časový úsek ako Download, Upload, Max. rýchlosť downloadu, Max rýchlosť Uploadu, IP adresy, verejné, lokálne a taktiež celkový súčet prenesených dát za celú sieť. Tlačidlo *Prenos cez porty* ponúka podrobný výpis prenosu dát jednotlivých programov cez nami zvolené porty s možnosťou zobrazenia do tabuľky alebo grafu. Zvyšné funkcie generovania výkazov budú podrobnejšie popísané v reportoch (4.3 Reporty).

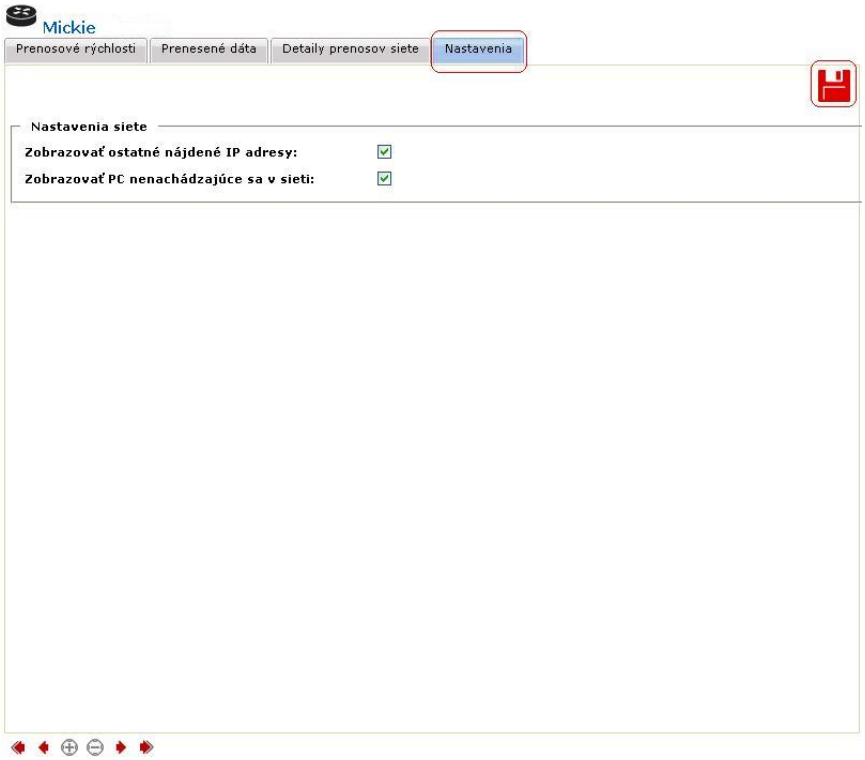


Obrázok č. 20 Detaily prenosov siete



Obrázok č. 21 Prenosy cez porty

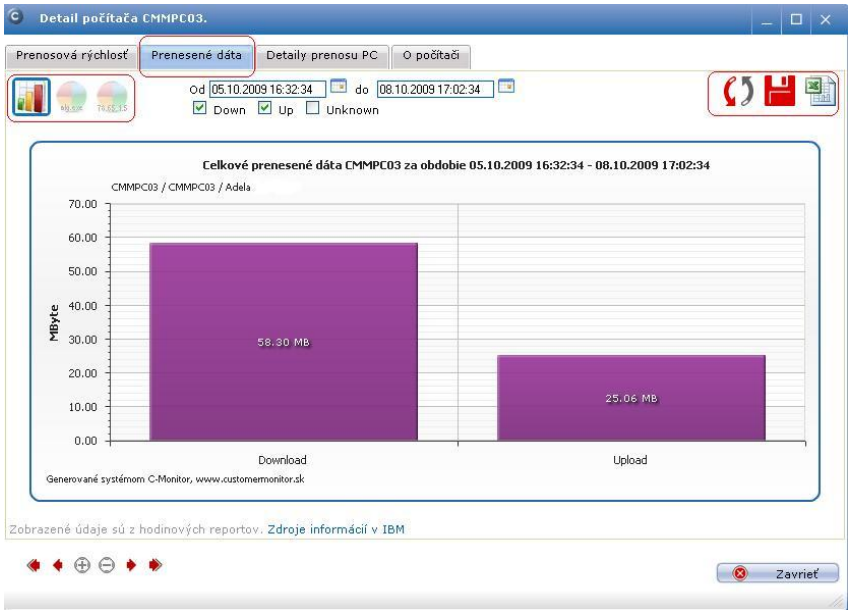
V záložke *Nastavenia* máme na výber nastaviť zobrazenie siete. Po výbere zobrazenia, klikneme na uložiť.



Obrázok č. 22 Nastavenia siete

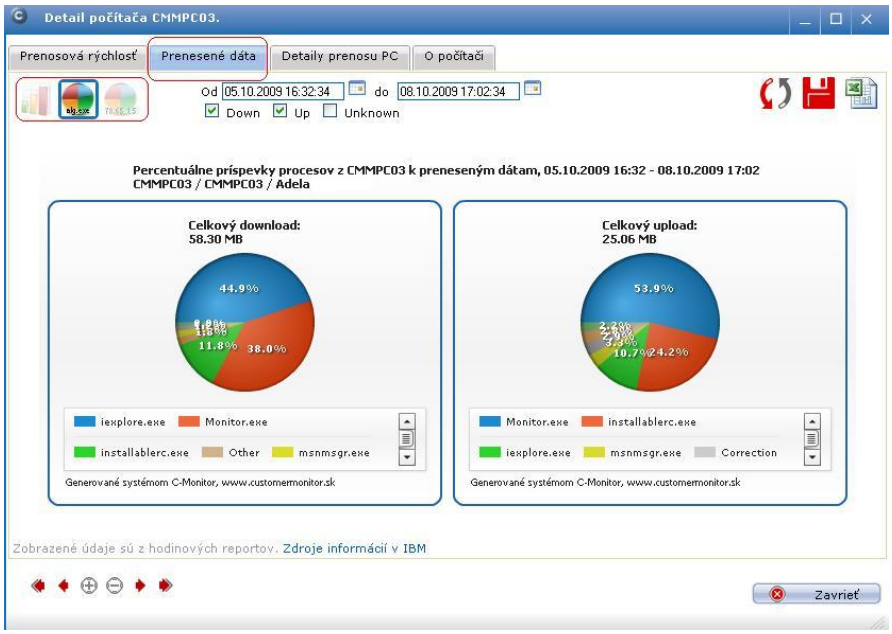
4.2.2 Prenesené dáta za konkrétny počítač

Prenesené dáta za konkrétny počítač zobrazíme kliknutím na počítač v topológii siete, v pravej časti obrázky a po kliknutí na záložku *Prenesené dáta*. Automaticky sa ako prvé otvorí *Stĺpcový graf* so zobrazením prenesených dát za nami zvolené obdobie.



Obrázok č. 23 Prenesené dáta za konkrétny PC

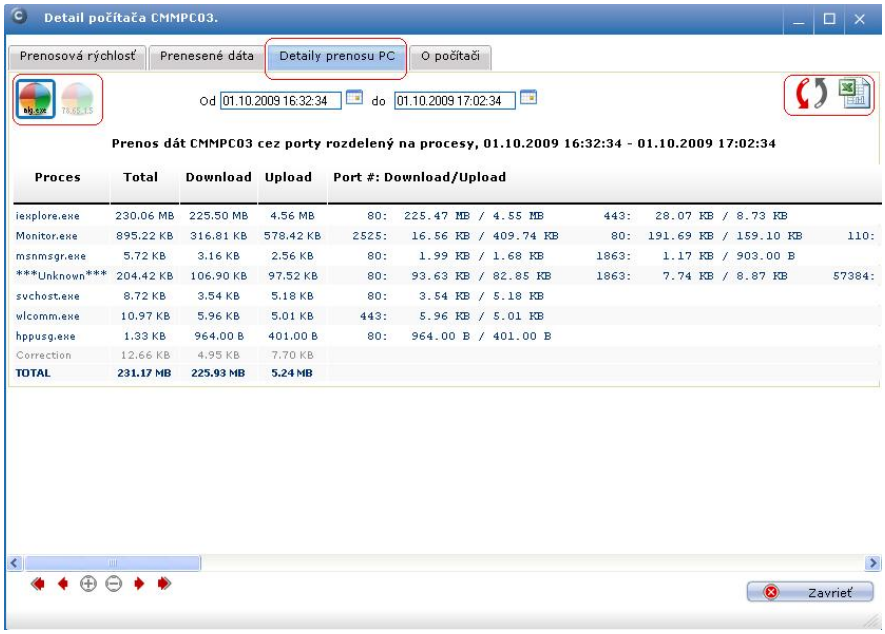
Ďalej je možnosť zobrazenia *Koláčového grafu* s percentuálnym podielom prenosov jednotlivých procesov a zobrazením prenosu na jednotlivé IP adresy.



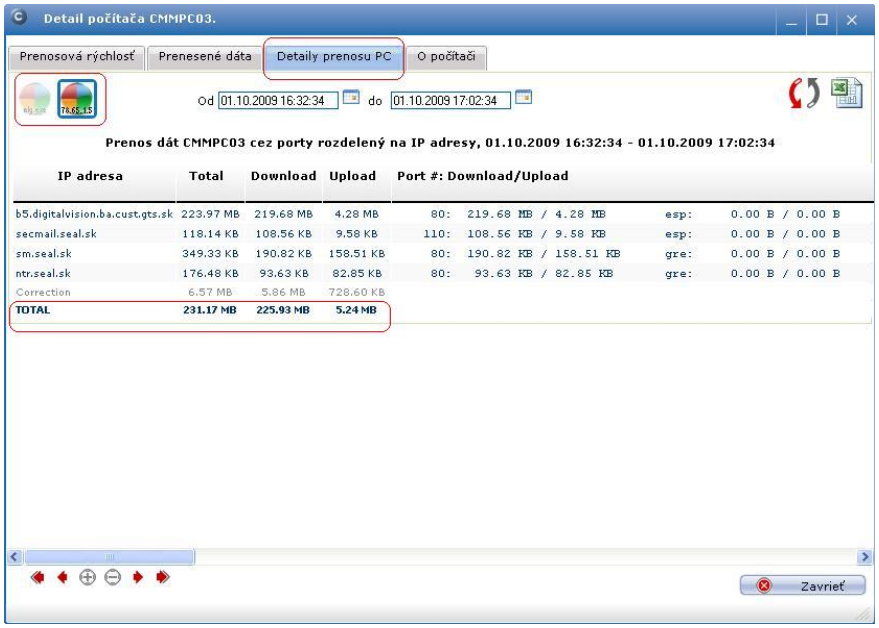
Obrázok č. 24 Percentuálne zobrazenie prenosu procesov

Obrázok č. 25 Percentuálne zobrazenie prenosu cez IP adresy

V záložke *Detaily prenosu PC*, máme na výber zobraziť podrobný zoznam procesov alebo IP adries a porty cez, ktoré komunikoval s množstvom prenesených dát za sledovaný časový interval. Všetky zobrazené štatistiky je možné vyexportovať do .png alebo .xls formátu.

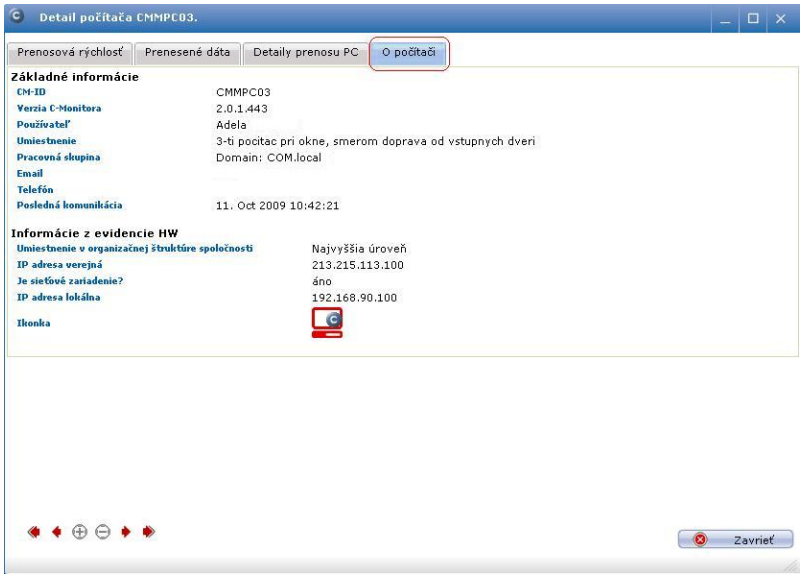


Obrázok č. 26 Zoznam procesov s množstvom prenesených dát



Obrázok č. 27 Zoznam IP adries s množstvom prenesených dát

V záložke *O počítači* máme uvedené základné informácie o vybranom PC.



Obrázok č. 28 Informácie o počítači

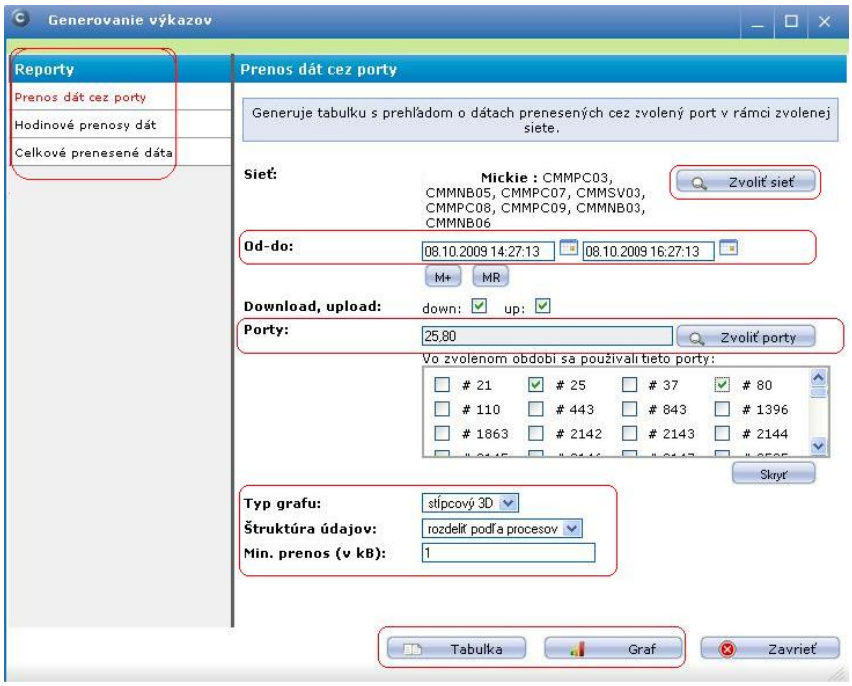
4.3 Reporty

Ponúkajú sumárny prehľad o prenose dát o sledovanej spoločnosti za nami vybrané obdobie s možnosťou exportovania údajov do známych formátov. Vieme zvoliť informácie o celej sieti ale aj za konkrétny počítač. Možnosti reportov sú cez horné menu *IBM ->Reporty* alebo v záložke *Detaily prenosov siete - > Prenosy cez porty*.
Možnosti reportov:

- Prenos dát cez porty
- Hodinové prenosy dát
- Celkové prenesené dáta
- Sumárny prehľad dní

4.3.1 Prenos dát cez porty

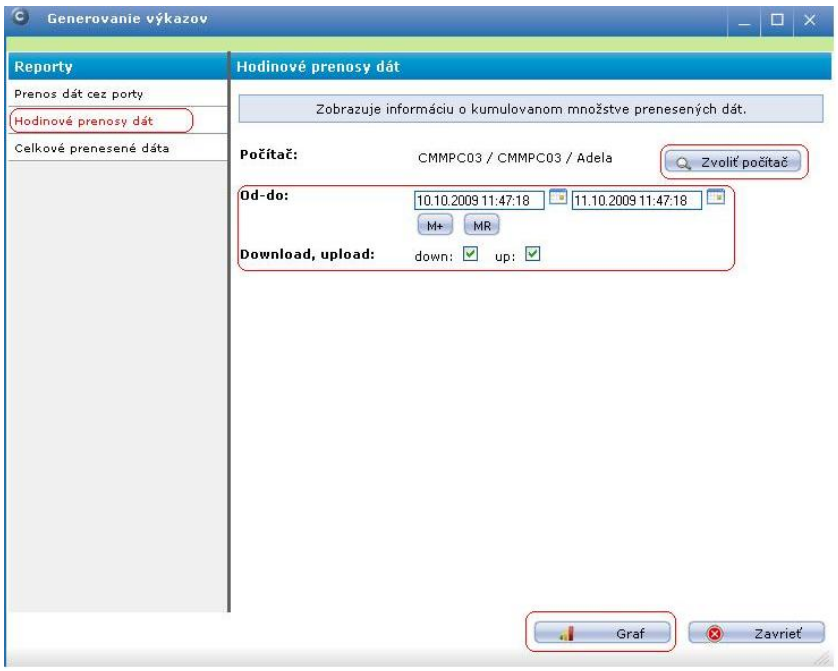
Ponúka detailný zoznam prenosov cez nami zvolené porty. Cez filter v pravej strane okna zvolíme požadované parametre ako sieť, ktorú sledujeme, časový interval, porty, typ grafu a zvolíme zobrazenie do tabuľky alebo grafu.



Obrázok č. 29 Prenos dát cez porty

4.3.2 Hodinové prenosy dát

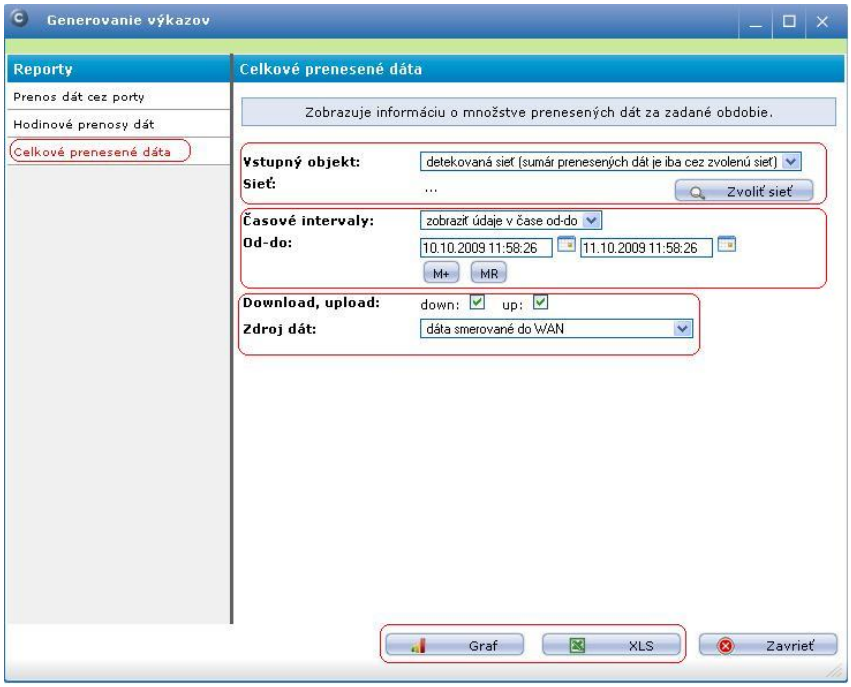
Ponúkajú informácie o prenesených dátach za vybraný počítač v hodinových intervaloch za požadované obdobie s možnosťou zobrazenia a uloženia grafu do obrázkového .png formátu.



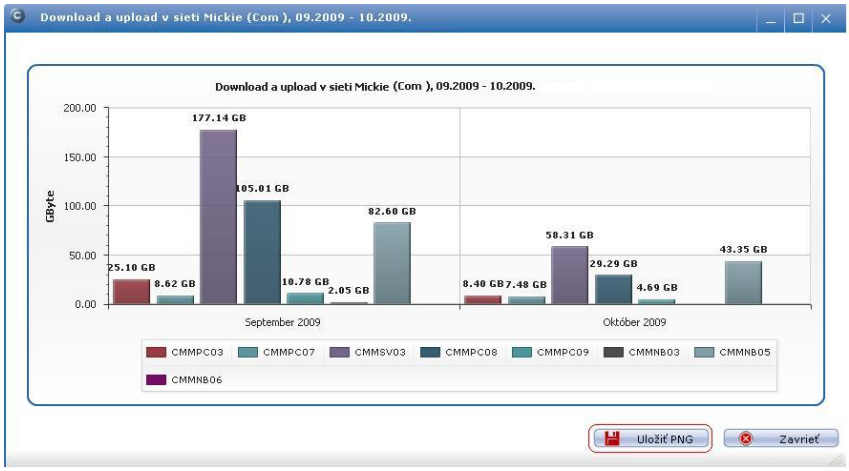
Obrázok č. 30 Hodinové prenosy dát

4.3.3 Celkové prenesené dáta

Vieme zobraziť informácie o množstve prenesených dát za celú sieť alebo konkrétny počítač v potrebnom časovom intervale. Ako prvé zvolíme *„Vstupný objekt“*, kde zvolíme sledovanie za celú sieť alebo vybraný počítač, v *„Časových intervaloch“* máme na výber zobraziť údaje v tvare od-do pre konkrétne dátumy alebo celé mesiace. V *„Zdroji dát“* máme na výber zvoliť zobrazenie dát smerovaných do WAN alebo všetky dáta prenesené cez sieťové adaptéry(teda aj prenos v rámci lokálnej siete). Výstup je buď zobrazenie do grafu s možnosťou uloženia do .png formátu alebo priamo do .xls formátu.



Obrázok č. 31 Celkové prenesené dáta



Obrázok č. 32 Grafický výstup celkového prenosu dát za dva mesiace