

Monitoring prenosených dát cez internet

verzia ku dňu 18.11.2009 a k verzii C-Monitoru 2.0.1.468



SEAL IT Services, s.r.o.



Obsah

<u>1 ÚVOD</u>	3
1.1 Úloha Monitoringu prenesených dát cez internet v CM 1.2 Upozornenie k možnosti blokácie sieťovej komunikácie	3 3
2 ZÁKLADNÝ PREHĽAD	5
 2.1 PRINCÍP FUNKČNOSTI	5 5 5 5 5
<u>3 DOPORUČOVANÁ ORGANIZÁCIA ZARIADENÍ V IBM</u> 3.1 Vstup do Internet Bandwith monitoringu (skratka IBM) 3.2 Automatická detekcia sietí 3.3 Akceptácia / Odmietnutie siete	7 7 7 8
3.4 VYTVORENIE SIEŤOVEJ VETVY, VLOŽENIE SIEŤOVÉHO PRVKU (V SW A HW EVIDENCII) 1	10
4 200 KAZENIE UDAJOV U INTERNETOVI CHI KENUSUCH NA SERVERI CM	<u></u>
 4.1 PREHĽAD PRENOSOV NA INTERNET ZA CELU SIET / VETVU V TOPOLOGII SIETE	4 6 7
4.2.2 PRENESENÉ DÁTA ZA CELO SIET	20 24 24
4.3.2 HODINOVÉ PRENOSY DÁT	25 26

CUSTOMER MONITOR

Manuál k monitorovaniu prenosu dát cez internet, verzia k 18.11.2009

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.

	Net Traffic Monitor
Dutgoing Messages SMTP 1 (for CM messages) SMTP 2 (for CM messages) MAPI Notification Messages SMTP 3 (for notif. messages) SMTP 4 (for notif. messages) ncomming Messages POP3 HTTP FTP Shared Folder Archive Customer Monitor Server (http)	 Monitor Network Traffic (only ethernet adapters) Separately Monitored Traffic IPs Disabled Adapte List of adapters, which should be excluded from network traffic monitoring, because they drivers are not compatible with CMonitor. Leadtek USB Network Interface Check Point Virtual Network Adapter
Remote Access Operators Security Easuclick Requests	

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 sieť ového 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 <u>nie je</u> 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.



:			
÷	9	Detekovan	_ X
		Neakceptovai	Internet bandwidth monitoring
÷	Ð	Detekovan	
T	-	Neakceptovai	Akceptovať sieť
÷	æ	Detekovan	Odmietnuť sieť
T .	9	Neakceptovai	
Ļ.	-	Detekovan	Rozbaľ všetko
(9	Neakceptovai	Zbaľ všetko
÷	Ð	Detekovan	Tlačiť
		меаксертоуак	a accelorana pres

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 "Premenovat".





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.

🙀 Vstupné údaje – SW Audit – HW Ev < Audit SW a evidencia HW	videncia Služby O 🔍 🍲	kno Rôzne	- Office, L	.INUX fir	ewall		
Topológia siete ⊡ 🏠 DS Družstvo	~	Vlastnosti ob	nosti objektu Sieťové porty Pôdorys				
Nitra - Office, LINUX f****** Mail server, ktorý je s Lokálna IP: 192.168.44, Pripo KooperuNetscreen Jur Lokálna IP: 192.168.44, Odpo Zara terminálová csarve	Topológia si Nitra - Office, LINU jené k: njiť k inému zariadeniu njiť (presunúť do neza diť do najvyššej úrovi	ete – × X firewall J pojených) 76	v organiza Automaticky	čnej štrukt • detekovana ¥lastnosť	úre spoločnos á sieť		
RNDPC01 / WIN-BACK Prem - Lokálna IP: 192.168.44 Vloži RNDPC01 / WIN-BACK Prem - Lokálna IP: 192.168.44 Zma RNDPC02 / RAKOVA / Zbali	ť nové zariadenie nenovať zať ť všetko	\supset					
E Kalna IP: 192.168.44. Rozb Rozbojené objekty Ilači Znov	aliť všetko ť vu načítať		zbierané IP adresy) nenachádzajúce sa v sieti				
Pozn.: v tomto strome sa zobrazujú iba majú nastavenú vlastnosť 'sieťové zaria	a zariadenia, ktoré adenie'.	Ikonka Zrkadlenie iko	onky				

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.



Switch v serverovom racku	<pre> [Port #3] [Port #4] [Port #5] [Port #6] [Port #7] [Port #8] [Port #9]</pre>	Zvolte výstupný port zariadenia na ľavej strane, ktorý sa má spojiť so vstupným portom zariadenia na pravej strane.	Port #1 — 🧾
	1	🖌 Prepojiť vybrané	porty 🛛 🔞 Zavrieť

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 vid". *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 \clubsuit \bigoplus \bigoplus \bigstar . Po zmene časového intervalu treba prekresliť graf nanovo stlačením tlačidla *Prekresliť graf* \checkmark 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



/ Bookmarks Iools Help ☆ (ⓒ https://sm.seal.sk/index2.php		☆・ अ• Google	R
*			-
1 19 100		CUSTO	NER MONITOR
n zóna <mark>Prehliadanie a Vyhodnotenie</mark> Custome	r Desk Pomac	Operátor : Milan	Odhlásiť
IBM Rôzne		🖵 Celá obrazovka	P Opustiť IBM
Spoločnosť Názov siete Pr	očítač & Umiestnenie Používateľ Operátor	Hľadaj	
rrnet Bandwidth Monitoring 🔹			
pológia siete	Prenosové rýchlosti Prenesené dáta Detaily prenosov siete Nastaveni	ia	
Com Mickie	od 08 10 2009 08 28 07 0 do 08 10 2009 10 28 07 0	M+ MB	5 💾 🖻
Verejná IPi 213,215,113,210 CMMPC03 / CMMPC03 / Adela			
Lokálna IP: 192.168.90.100 08. Oct 2009 10:27:51	C		
Aktivita mail spojenia: PASSIVE CMMNB05 / IBM-DIANA / diana	Celková prenosová rýchlosť (down + up) v Mickie(Com od 08.10.2009 08:28:07 do 08.10.2009 10:28:07.	n)	
Lokálna IP: 192.168.90.111 08. Oct 2009 10:27:57	70.0]		_
Aktivita mail spojenia: PASSIVE CMMPC07 / CMMPC07 / Katarina	60.0		
Lokálna IP: 192.168.90.103 08. Oct 2009 10(27)49	500	*	
CMMSV03 / COMMSERVER / server	30.0		
Lokina IP: 192.168,90.5	ू 40.0 भू		_
Aktivita mail spojenia: PASSIVE CMMPC08 / CMMPC08 / Alexandra	£ 30.0 -	A	
Lokálna IP: 192:168:90.107	20.0	1/1 1	_
Aktivita mail spojenia: PASSIVE CMMPC09 / COMPC09 / Maria	10.0		
Lokalna IP/ 192.168.90.105 08. Oct 2009 10:27:52	a constant of a	MANIA	la.
Aktivita mail spojenia: PASSIVE CMMNB03 / CMMNB03 / agenturny	08.10.2009 08.10.2009 08.10.2009 08.10.2009 08.10.2009	08.10.2009 08.10.2009 08.10.2009	08.10.2009
notebook na prezentacie Lokálna IPr 192.168.90.108	08:29:00 08:44:00 08:59:00 09:14:00 09:29:00	09:44:00 09:59:00 10:14:00	10:29:00
Aktivita mail spojenia: PASSIVE CMMNB06 / MIRKA-VAIO13 / Miroslava	Total / CMMPC03 / CMMPC03 / Adela		
- Lokálna IP: 192.168.90.108	CMMSV03 / COMSERVER / server Win2003 SBS, bez pr	racovnika	
20: Aug 2009 15:08:56 Aktivita mail spojenia: PASSIVE	CMMPC07 / CMMPC07 / Katarina / CMMPC	08 / CMMPC08 / Alexandra	
The mill contract of a finder of the advances		15 / IBM-DIANA / diana	

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 <u>celkový súčet prenesených dát za celú sieť</u>. Tlačidlo *Prenos cez porty* ponúka podrobný výpis prenosu dát jednotlivých programov cez nami zvolené porty s možnosť ou zobrazenia do tabuľky alebo grafu. Zvyšné funkcie generovania výkazov budú podrobnejšie popísané v reportoch (4.3 Reporty).

renosové	rýchlosti Pre	nesené dáta 🛛 🛛	etaily prend	osov siete	Nastav	enia			
enesené (Všeobe	dáta od 08.10.200 cné informácie	9 14:03:07	d 08.10.2009	16:03:07	M+	MR			()
1AC adro P adres	esa gateway: 0 a gateway: 192	0:04:23:31:9B:24 .168.90.1							
Prenes	ené dáta 8. Oct	2009 14:03:07	- 8. Oct 20	09 16:03:	07 —				57755. 185743
CM-ID ⊞	Počítač	Používateľ	Down	Up	Total	Max. rýchlosť Down	Max. rýchlosť Up	IP verejná	IP lokálne
CMMNB03	CMMNB03	agenturny notebook na prezentacie	0.00 B	0.00 B	0.00 B	0.00 B	0.00 B	213.215.113.210	192.168.90.108
CMMNB05	IBM-DIANA	diana	2.94 MB	688.55 KB	3.62 MB	7.15 KB	805.80 B	213.215.113.210	192.168.90.111
CMMNB06	MIRKA-VAIO13	Miroslava	0.00 B	0.00 B	0.00 B	0.00 B	0.00 B	213.215.113.210	192.168.90.108
	CMMPC03	Adela	3.18 MB	596.45 KB	3.76 MB	7.15 KB	321.30 B	213.215.113.210	192.168.90.100
CMMPC07	CMMPC07	Katarina	4.40 MB	710.14 KB	5.09 MB	79.77 KB	3.33 KB	213.215.113.210	192.168.90.103
	CMMPC08	Alexandra	588.36 KB	408.95 KB	997.31	160.60 B	87.47 B	213.215.113.210	192.168.90.107
	COMPC09	Maria	8.53 MB	1.29 MB	9.82 MB	15.95 KB	2.39 KB	213.215.113.210	192.168.90.105
CMMS¥03	COMSERVER	server Win2003 SBS, bez pracovnika	1.55 MB	21.53 MB	23.08 MB	2.60 KB	53.12 KB	213.215.113.210	192.168.90.5
Tetal 08.10.200	9 14:03:07 - 08.1	0.2009 16:03:07	21.17 MB	25.17 MB	46.34 MB	79.77 KB	53.12 KB		
4	rendsy cez porty								

Obrázok č. 20 Detaily prenosov siete

eporty	Prenos dát cez porty	
enos dát cez porty odinové prenosy dát	Generuje tabulku s pre	zhľadom o dátach prenesených cez zvolený port v rámci zvoler siete.
elkové prenesené dáta	Sieť:	Mickie: CMMPC03, CMMNB05, CMMPC07, CMMSV03, CMMPC08, CMMPC09, CMMNB03, CMMNB06
	Od-do:	08.10.2009 14:27:13 (08.10.2009 16:27:13)
	Download, upload:	down: 🗹 up: 🗹
	Porty:	25,80 Q. Zvoliť porty
		Vo zvolenom obdobi sa používali tieto porty: # 21 # 25 # 37 # # 80 # 110 # 443 # 843 # 1396 # 1863 # 2142 # 2143 # 2144 # 0000 # 0000 # 0000 # 0000 # 1863 # 2142 # 2143 # 2144
	Typ grafu: Štruktúra údajov: Min. prenos (v kB):	stípcový 3D V rozdelíř podľa procesov V 1

Obrázok č. 21 Prenosy cez porty



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

renosové rýchlosti	Prenesené dáta	Detaily prenosov :	siete Nastavenia	
Nastavenia siete				
Zobrazovať ostati	né nájdené IP adro	esy: 🗹		
Zobrazovať PC ne	nachádzajúce sa v	v sieti: 🗹		

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.

renosová rýchlosť Prenesené dáta Detaily prenosu PC O poč Od 05.10.2003 16.32:34 do 08.10.2003 V Down V Up Unknown	Sitadi 117.02:34 🔲 🎧 🎦 📲
Percentuálne príspevky procesov z CMMPCO3 k prenes CMMPCO3 / CMMPCO3 / Adela	seným dátam, 05.10.2009 16:32 - 08.10.2009 17:02
Celkový download: 58.30 MB	Celkový upload: 25.06 MB
44,9% 【最終 11.8% 38.0%	53.9% 338 10.7%24.2%
iexplore.exe Monitor.exe	Monitor.exe 📕 installablerc.exe
📕 installablerc.exe 📕 Other 📕 msnmsgr.exe 📕	📕 iexplore.exe 📒 msnmsgr.exe 📰 Correction 📱
Generované systémom C-Monitor, www.customermonitor.sk	Generované systémom C-Monitor, www.customermonitor.sk
brazené údaje sú z hodinových reportov. Zdroje informácií v IBM	

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.



Od [01.10.2009 16:32:34] Image: Description of the second sec	Prenosova rycr	niost Pre	nesene data	Detally	prenosu PC	U poc	itaci							
Prenos dát CMMPCO3 cez porty rozdelený na procesy, 01.10.2009 16:32:34 - 01.10.2009 17:02:34 Proces Total Download Upload Port #: Download/Upload Monitor.exe 295.02 KB 25.50 MB 4.56 MB 80: 225.47 MB / 4.55 MB 443: 28.07 KB / 8.73 KB Monitor.exe 895.22 KB 316.81 KB 578.42 KB 2525: 16.56 KB / 409.74 KB 80: 191.69 KB / 158.10 KB 111 msnmsgr.exe 5.72 KB 3.16 KB 2.56 KB 80: 1.99 KB / 1.68 KB 1063: 1.17 KB / 903.00 E ***Unknown*** 204.42 KB 106.90 KB 97.52 KB 80: 3.64 KB / 5.18 KB 80: 3.64 KB / 5.18 KB 60: 964.00 B / 401.00 B <			Od 01.10.2	2009 16:32:34	do 📼	01.10.2009	17:02	34) 🖭
Best Point Server 230.06 MB 225.50 MB 4.56 MB 80: 225.47 MB / 4.55 MB 443: 28.07 KB / 8.73 KB Monitorexe 895.22 KB 316.81 KB 578.42 KB 2525: 16.56 KB / 409.74 KB 80: 191.69 KB / 159.10 KB 111 mannsgrexe 5.72 KB 3.16 KB 275.42 KB 2525: 16.56 KB / 409.74 KB 80: 191.69 KB / 159.10 KB 111 mannsgrexe 5.72 KB 3.16 KB 275.42 KB 80: 1.99 KB / 1.68 KB 1863: 1.17 KB / 903.00 E ***Unknown*** 204.42 KB 106.90 KB 97.52 KB 80: 3.54 KB 80: 3.54 KB 5.18 KB 80: 3.54 KB 5.96 KB 5.01 KB 443: 5.96 KB 7.70 KB 443: 5.96 KB 5.96 KB 7.70 K	Proces	Prenos dá Total	t CMMPC03 Download	cez porty Upload	rozdelený Port #: D	na proce ownload/	uplc	01.10.2009 1 oad	6:32:34 -	01.10.20	09 1	7:0	2:34	
Monitor.exe 895.22 KB 316.81 KB 578.42 KB 2525: 16.56 KB / 409.74 KB 80: 191.69 KB / 159.10 KB 111 msnmsgr.exe 5.72 KB 3.16 KB 2.56 KB 80: 1.99 KB / 1.68 KB 1663: 1.17 KB / 903.00 E ***Unknown*** 204.42 KB 106.90 KB 97.52 KB 80: 3.93 KB / 82.85 KB 1863: 7.74 KB / 9.87 KB 5738 svchost.exe 8.72 KB 5.96 KB 5.18 KB 80: 3.54 KB / 5.18 KB 80: 3.54 KB / 5.18 KB 7.74 KB / 9.87 KB 5738 svchost.exe 8.72 KB 5.96 KB 5.01 KB 443: 5.96 KB / 5.01 KB 443: 5.96 KB / 5.01 KB 443: 5.96 KB / 5.01 KB 441: 5.96 KB / 401:00 B 5.24 KB	iexplore.exe	230.06 MB	225.50 MB	4.56 MB	80:	225.47	MB /	4.55 MB	443:	28.07	KB	/ 8.	73 KB	
msnmsgr.exe 5.72 KB 3.16 KB 2.56 KB 90: 1.99 KD / 1.68 KB 1863: 1.17 KB / 903.00 B ***0uhnovn*** 204.42 KB 106.90 KB 97.52 KB 80: 93.63 KB / 82.85 KB 1863: 7.74 KB / 8.87 KB 5738 svchost.exe 8.72 KB 3.54 KB 5.18 KB 80: 3.54 KB / 5.18 KB 1067 KB 7.74 KB / 8.87 KB 5738 ulconm.exe 10.97 KB 5.96 KB 5.01 KB 401.00 B 80: 964.00 B / 401.00 B hppusg.exe 1.33 KB 964.00 B 401.00 B 80: 964.00 B / 401.00 B correction 12.66 KB 4.95 KB 7.70 KB 70 KB TOTAL 231.17 MB 225.93 MB 5.24 MB	Monitor.exe	895.22 KB	316.81 KB	578.42 KB	2525:	16.56	KB /	409.74 KB	80:	191.69	KB	/ 18	59.10 KB	110
****Unknown*** 204.42 KB 106.90 KB 97.52 KB 90: 93.63 KD / 82.85 KB 1063: 7.74 KD / 8.87 KB 5738- svchotseve 8.72 KB 3.54 KB 5.18 KB 80: 3.54 KD / 5.18 KB wlcomm.exe 10.97 KB 5.96 KB 5.01 KB 443: 5.96 KB / 5.01 KB pourge.exe 1.33 KB 54.000 B 401.00 B 60: 364.00 B / 401.00 B Correction 12.66 KB 4.95 KB 7.70 KB 7.70 KB 70 KB TOTAL 231.17 MB 225.93 MB 5.24 MB 5.24 MB 5.24 MB	msnmsgr.exe	5.72 KB	3.16 KB	2.56 KB	80:	1.99	KB /	1.68 KB	1863:	1.17	KB	/ 90	03.00 B	
svchostexe 8.72 KB 3.54 KB 5.18 KB 80: 3.54 KB / 5.18 KB wlcomm.exe 10.97 KB 5.96 KB 5.01 KB 443: 5.96 KB / 5.01 KB hppusg.exe 1.33 KB 964.00 B 401.00 B 80: 964.00 B / 401.00 B Correction 12.66 KB 4.95 KB 7.70 KB TOTAL 231.17 MB 225,93 MB 5.24 MB	***Unknown***	204.42 KB	106.90 KB	97.52 KB	80:	93.63	KB /	82.85 KB	1863:	7.74	KB	/ 8.	87 KB	57384
vlcomm.exe 10.97 KB 5.96 KB 5.01 KB 443: 5.96 KB / 5.01 KB nppusg.exe 1.33 KB 964.00 B 401.00 B 80: 964.00 B / 401.00 B Correction 12.66 KB 4.95 KB 7.70 KB TOTAL 231.17 MB 225,93 MB 5.24 MB	svchost.exe	8.72 KB	3.54 KB	5.18 KB	80:	3.54	KB /	5.18 KB						
hppusg.exe 1.33 KB 964.00 B 401.00 B 80: 964.00 B / 401.00 B Correction 12.66 KB 4.95 KB 7.70 KB TOTAL 231.17 MB 225.93 MB 5.24 MB	wlcomm.exe	10.97 KB	5.96 KB	5.01 KB	443:	5.96	KB /	5.01 KB						
Correction 12.66 KB 4.95 KB 7.70 KB TOTAL 231.17 MB 225,93 MB 5.24 MB	hppusg.exe	1.33 KB	964.00 B	401.00 B	80:	964.00	в /	401.00 B						
TOTAL 231.17 MB 225.93 MB 5.24 MB	Correction	12.66 KB	4.95 KB	7.70 KB										
	TOTAL	231.17 MB	225.93 MB	5.24 MB										
	Correction TOTAL	12.66 KB 231.17 MB	4.95 KB 225.93 MB	7.70 KB 5.24 MB		564.00	<i>b</i> /	401.00 5						

Obrázok č. 26 Zoznam procesov s množstvom prenesených dát

Prenosová rýchlosť Pre	enesené dát	a Detaily	prenosu PC	O počít	tači			
112 Sam (78.65.15)	Od 01.1	0.2009 16:32:34	1 🗾 do	01.10.2009 1	17:02:34		ç) 🖻
Prenos dá IP adresa	t CMMPC03 Total	cez porty i Download	·ozdelený Upload	na IP adre Port #: D	esy, 01.10.2009 16:32:34 - ownload/Upload	01.10.2009	0 17:02:34	
b5.digitalvision.ba.cust.gts.sk	223.97 MB	219.68 MB	4.28 MB	80:	219.68 MB / 4.28 MB	esp:	0.00 B / 0	.00 B
secmail.seal.sk	118.14 KB	108.56 KB	9.58 KB	110:	108.56 KB / 9.58 KB	esp:	0.00 B / 0	.00 B
sm.seal.sk	349.33 KB	190.82 KB	158.51 KB	80:	190.82 KB / 158.51 KB	gre:	0.00 B / 0	.00 B
ntr.seal.sk	176.48 KB	93.63 KB	82.85 KB	80:	93.63 KB / 82.85 KB	gre:	0.00 B / 0	.00 B
Correction	6.57 MB	5.86 MB	728.60 KB					
TOTAL	231.17 MB	225.93 MB	5.24 MB	(à				

Obrázok č. 27 Zoznam IP adries s množstvom prenesených dát



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

Prenosová rýchlosť	Prenesené dáta	Detaily prenosu PC	O počítači			
ákladné informácie						
CM-ID	CMM	IPC03				
Verzia C-Monitora	2.0.1.443					
Používateľ	Adela					
Umiestnenie	3-ti p	pocitac pri okne, smero	m doprava od vstupnych dveri			
Pracovná skupina	Dom	ain: COM.local				
Email						
Telefón						
Posledná komunikácia	11. 0	Oct 2009 10:42:21				
Informácie z eviden	cie HW					
Umiestnenie v organizačnej štruktúre spoločnosti		sti Najvyššia	úroveň			
IP adresa verejná		213.215.113.100				
Je sieťové zariadenie?		áno				
IP adresa lokálna	aa 192.168.90.1		0.100			
These is		C				
IRONRA						
	12					
4 4 0 0 4						

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.

Reporty	Prenos dát cez porty		
Prenos dát cez porty Hodinové prenosy dát	Generuje tabulku s pre	hľadom o dátach prenesených cez zvolený port v rámci zvolene, siete.	
Celkové prenesené dáta	Sieť:	Mickie : CMMPC03, CMMNB05, CMMPC07, CMMSV03, CMMPC08, CMMPC09, CMMNB03, CMMNB06	
	Od-do:	08.10.2009 14:27:13	
	Download, upload:	down: ☑ up: ☑	
	Porty:	25,80 Q. Zvoliť porty	
		Vo zvolenom obdobi sa použivali teto porty: # 21 # # 25 # 37 # # 80 # 110 # 443 # 843 # 1396 # 1863 # 2142 # 2143 # 2144	
	Typ grafu: Štruktúra údajov: Min. prenos (v kB):	stípcový 3D V rozdeliť podľa procesov V 1	

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.

G Generovanie výkazov – 🗧			
Reporty	Hodinové prenosy dát		
Prenos dát cez porty Hodinové prenosy dát Celkové prenesené dáta	Zobrazuje informáciu o kumulovanom množstve prenesených dát.		
	Počítač:	CMMPC03 / CMMPC03 / Adela	
	Od-do:	10.10.2009 11:47:18 11.10.2009 11:47:18 MR	
	Download, upload:	down: 🗹 up: 🗹	
		Graf Savrieť	

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 sieť ové adaptéry(teda aj prenos v rámci lokálnej siete). Výstup je buď zobrazenie do grafu s možnosť ou uloženia do .png formátu alebo priamo do .xls formátu.

Reporty	Celkové prenesené dáta Zobrazuje informáciu o množstve prenesených dát za zadané obdobie.		
Prenos dát cez porty Hodinové prenosy dát			
(Celkové prenesené dáta)	¥stupný objekt: Sieť:	detekovaná sieť (sumár prenesených dát je iba cez zvolenú sieť) 🗸	
	Časové intervaly: Od-do:	zobrazř údaje v čase od-do ▼ 10.10.2009 11:58.26 ■ M# MR	
	Download, upload: Zdroj dát:	down: ☑ up: ☑ dáta smerované do WAN	

Obrázok č. 31 Celkové prenesené dáta



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



