Nástroje pro analýzu

počítačových sítí

Šárka Vavrečková

Ústav informatiky, FPF SU Opava

sarka.vavreckova@fpf.slu.cz

Poslední aktualizace: 4. prosince 2014

Informace o podezřelém e-mailu

Průzkum zdrojového kódu e-mailu

- Thunderbird: Ctrl+U nebo Zobrazení-Zdrojový kód stránky, jinak obvykle někde v kontextovém menu
- protokol SMTP pro zasílání e-mailů je textově orientovaný (ne binární), takže se zprávy snadno zkoumají

Popis některých položek:

http://www.computerhope.com/issues/ch000918.htm

Co se dá zjistit

1. Adresy uzlů, přes které zpráva šla

- seznam adres uzlů:
  - na začátku zprávy je seznam těchto adres s dalšími údaji
  - každý uzel přidá svou adresu za začátek tohoto seznamu (tj. princip „zásobník“)
  - IP adresu odesílatele najdeme až na konci tohoto seznamu
- několik typů uzlů:
  - Delivered-To: adresát@doména.cz
    - komu byla zpráva doručena (hned první adresa v seznamu, přidána jako poslední)
  - Received: by/from xxxxx (další údaje) for adresát@doména.cz
    - vícekrát (každý takový záznam přes několik řádků), pro každý uzel na cestě
  - další

Co se dá zjistit

2. Metainformace o zprávě

- Message-Id: <identifikátor odesílané zprávy@odesílatel.xxx>
- To: adresát@doména.cz
- From: odesílatel@doména.cz
- Reply-To: kam se má poslat odpověď
- Return-Path: když nastane chyba, kam podat zprávu
- Date: xxxxx
- MIME-Version: 1.0 (verze protokolu pro typ obsahu)
- Content-Type: typ obsahu (např. text/plain, text/html, multipart/alternative, multipart/related, atd.) s parametry
- Subject: předmět zprávy

Průzkum zdrojového kódu zprávy

viz samostatný soubor

Konverzace s SMTP serverem

Klient se připojí k SMTP serveru na portu 25

- 220 staff.uiuc.edu ESMTP Sendmail 8.10.0/8.10.0 ready; Mon, 13 Mar 2000 14:54:08 -0600
  helo students.uiuc.edu
- 250 staff.uiuc.edu Hello root@students.uiuc.edu [128.174.5.62], pleased to meet you
  mail from: johndoe@students.uiuc.edu
- 250 2.1.0 johndoe@students.uiuc.edu... Sender ok
  rcpt to: jsmith@staff.uiuc.edu
- 250 2.1.5 jsmith@staff.uiuc.edu... Recipient ok
  data

- 354 Enter mail, end with "." on a line by itself

```
Received: (from johndoe@localhost)
  by students.uiuc.edu (8.9.3/8.9.3) id LAA05394;
  Mon, 5 Jul 1999 23:46:18 -0500
Date: Mon, 5 Jul 1999 23:46:18 -0500
From: John Doe <johndoe@students.uiuc.edu>
To: John Smith <jsmith@staff.uiuc.edu>
Message-Id: <199907052346.LAA05394@students.uiuc.edu>
Subject: This is a subject header.

This is the message body. xxxxxx

.
```

- 250 2.0.0 e2DKuDw34528 Message accepted for delivery

```
quit
```

- 221 2.0.0 staff.uiuc.edu closing connection

Analýza záhlaví mailu

Message Header Analyzer

https://toolbox.googleapps.com/apps/messageheader/

- vložím zdrojový kód mailu
- mohu zobrazit stručnou analýzu hlavičky

Email Header Analyzer

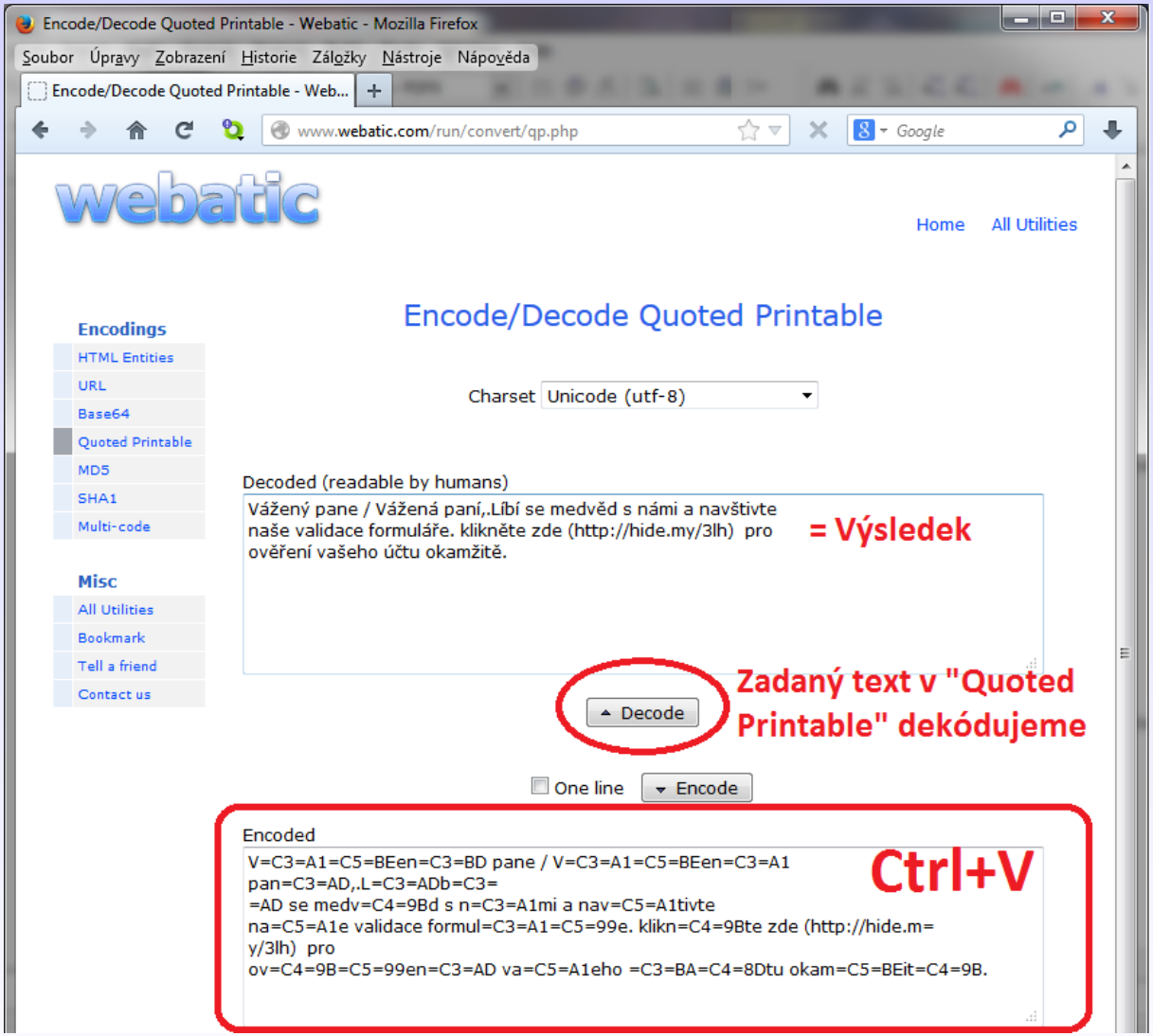
http://mxtoolbox.com/EmailHeaders.aspx

- vložím zdrojový kód mailu
- mohu zobrazit podrobnější analýzu hlavičky

Zprávy text/plain a text/html

Dekódování

- většinou je použito kódování „Quoted Printable“ (zajišťuje, aby bylo možné bez problémů přenášet texty jako sekvenci 7bitových znaků)
- potřebujeme přeložit do čitelnějšího formátu, např.:
  `V=C3=A1=C5=BEen=C3=BD pane` $\Longrightarrow$ `Vážený pane`
- http://www.webatic.com/run/convert/qp.php


Encode/Decode Quoted Printable - Webatic - Mozilla Firefox
Soubor Úpravy Zobrazení Historie Záložky Nástroje Nápověda
Encode/Decode Quoted Printable - Web...
www.webatic.com/run/convert/qp.php
Google
webatic
Home
All Utilities
Encodings
HTML Entities
URL
Base64
Quoted Printable
MD5
SHA1
Multi-code
Misc
All Utilities
Bookmark
Tell a friend
Contact us
Encode/Decode Quoted Printable
Charset Unicode (utf-8)
Decoded (readable by humans)
Vážený pane / Vážená paní,.Líbí se medvěd s námi a navštivte naše validace formuláře. klikněte zde (http://hide.my/3lh) pro ověření vašeho účtu okamžitě.
= Výsledek
Decode
Zadaný text v "Quoted Printable" dekódujeme
One line
Encode
Encoded
V=C3=A1=C5=BEen=C3=BD pane / V=C3=A1=C5=BEen=C3=A1 pan=C3=AD,.L=C3=ADb=C3= =AD se medv=C4=9Bd s n=C3=A1mi a nav=C5=A1tivte na=C5=A1e validace formul=C3=A1=C5=99e. klikn=C4=9Bte zde (http://hide.m= y/3lh) pro ov=C4=9B=C5=99en=C3=AD va=C5=A1eho =C3=BA=C4=8Dtu okam=C5=BEit=C4=9B.
Ctrl+V

Kdo je vlastníkem domény?

Kdy například zjišťujeme:

- když chceme registrovat vlastní doménu a ověřujeme, jestli už není registrovaná
- když z určité adresy přichází spam či malware a chceme zjistit odpovědnost, upozornit

Kdo je vlastníkem domény?

Mechanismus WHOIS v Linuxu

- `whois slu.cz`
- `whois -r slu.cz`
- další přepínače viz manuálové stránky – `man whois`
  - vyžádali jsme si informaci přímo z RIPE databáze (RIPE je jeden z pěti hlavních světových registrátorů domén – pro Evropu)

Kdo je vlastníkem domény?

Co můžeme dělat, když nemáme Linux?

WHOIS databáze jsou dostupné i na internetu

- zeptáme se Googlu – whois
- https://apps.db.ripe.net/search/query.html (RIPE – domény v rámci Evropy)
- http://whois.net/
- http://www.nic.cz/whois/ (český registrátor domén)

Jak funguje ARP

- ARP tabulka uchovává informace o sousedech (obvykle dvojice IP adresa + MAC adresa)
- je to bezstavový protokol, reaguje vždy na poslední dotaz nebo požadavek, nepamatuje si, co bylo předtím
- chci zjistit MAC adresu počítače s určitou IP adresou, vyšlu ARP rámec s dotazem:
  `arp who-has neznámáIP tell mojeIP`
  počítač, který pozná svou IP, odpoví s informací o své MAC:
  `arp reply jehoIP is-at jehoMAC`
- záznamy se dají jednoduše podvrhnout

ARP cache poisoning

- útok na ARP cache („otrávení ARP“)
- útočník chce přijímat provoz určený jinému zařízení:
  - pravidelně rozesílu podvržené ARP odpovědi s informací
  - jeho (podvržená) IP adresa a MAC adresa oběti
- útočník chce obousměrně monitorovat provoz mezi počítači A a B:
  - v ARP tabulce počítače A podvrhne záznam, že IP adresa počítače B se má mapovat na jeho MAC adresu
  - v ARP tabulce počítače B podvrhne záznam, že IP adresa počítače A se má mapovat na jeho MAC adresu

ARP cache poisoning

Jak se bránit

- program ARPWatch – pro Linux a teď i pro Windows, ARP Monitor
- přidává stavové chování, hlídá změny směrování záznamů v ARP tabulce
- problém: v síti se switchem nebo routerem „nevidí“ všechny ARP dotazy a odpovědi, ale jen to, co je zasíláno přímo na daný počítač
- řešení: buď instalujeme na všechny stanice, anebo použijeme centrální logování (syslog nebo něco podobného) pro ARP
- další obrana: statické ARP tabulky

Změna MAC adresy síťového zařízení

- když útočník chce odposlouchávat pakety určené pro jiné zařízení, může změnit svou MAC adresu na MAC adresu tohoto zařízení

$\Rightarrow$ v síti jsou dvě zařízení se stejnou MAC adresou, switch má v CAM/MAC tabulce tytéž adresy u dvou portů

- switche můžou na takovou situaci reagovat různě:
  - předávat provoz na oba porty
  - předávat buď na jeden nebo na druhý port (i náhodně)
  - nepředávat na žádný port
  - něco z předchozích + hlásit chybu
- obrana: na chybová hlášení reagovat; některé switche poskytují funkci „zabezpečení portu“, která detekuje všechny možné reakce

Jak se dá změnit MAC adresa

v Linuxu:

- starší způsob:

```
ifconfig eth0 down hw ether 02:00:00:00:11:22
ifconfig eth0 up
```

- novější způsob:

```
ip link set dev eth0 down
ip link set dev eth0 address 02:00:00:00:11:22
ip link set dev eth0 up
```

Jak se dá změnit MAC adresa

ve Windows:

- Správce zařízení (dostaneme se k němu i v konzole Správa počítače – pravé tlačítko myši na Počítač, položka Spravovat)
- najdeme Síťové adaptéry, zvolíme ten, který potřebujeme
- Vlastnosti nebo poklepat
- záložka Upřesnit, volba Síťová adresa (ale může tam být i jiná položka obsahující řetězec „adresa“), vpravo zadáme MAC adresu bez oddělovačů, hexadecimálně, velká písmena
- ta položka tam vůbec nemusí být
- riziková operace
- další možnost: změna v registru

Promiskuitní režim síťového rozhraní

- normální režim: síťové rozhraní přijímá pouze ty pakety, které
  - jsou určeny přímo pro toto rozhraní (jeho adresa je jako cílová)
  - broadcast, multicast apod.

  ostatní zahazuje
- promiskuitní režim: síťové rozhraní přijímá všechny pakety, žádný nezahazuje
- režim přeposílání (forwarding): pro mezilehlá zařízení (switch apod.)

Promiskuitní režim síťového rozhraní

K čemu je to dobré

- pro útočníka: možnost získat některé informace bez nutnosti ARP cache poisoning (například ARP a DHCP požadavky)
- pro správce sítě: možnost sledovat provoz a odhalovat technické problémy v síti, resp. nelegální provoz

Pokud má v síti běžet sniffer (program pro odposlouchávání provozu – také od správce sítě), je na zařízení běžícím v promiskuitním režimu, anebo použijeme některou z metod napojení se na provoz).

Odhalení rozhraní v promiskuitním režimu

- program *sniffdet* (Remote Sniffer Detector) – pro Linux

Jak se to dá nastavit

v Linuxu:

- `ipconfig eth0 promisc`
- `ip link set eth0 promisc on`

ve Windows:

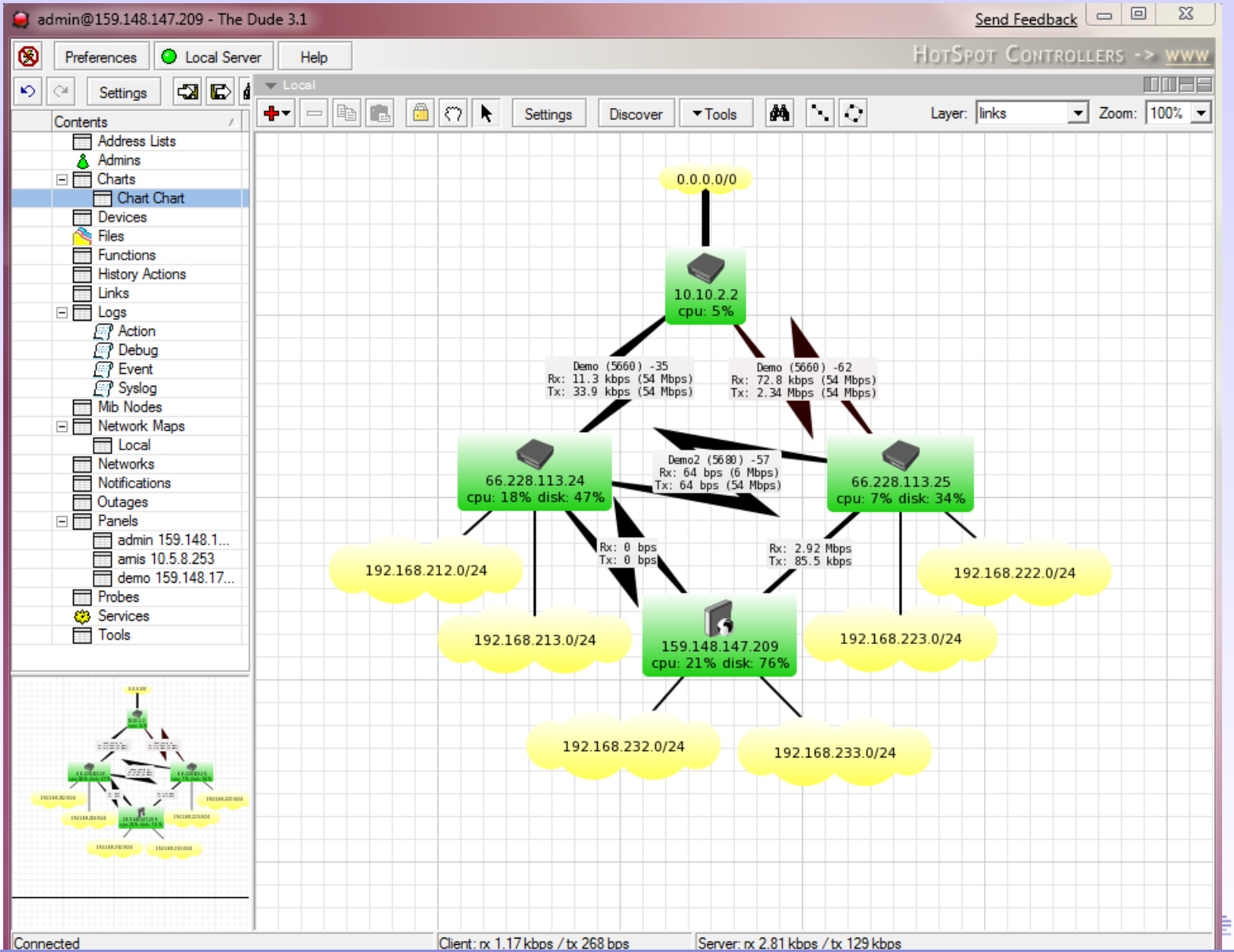
- jde to přes NetShell (prostředí spustíme příkazem `netsh`)
- lepší možnost: použít některý vhodný nástroj, ve kterém tento režim využijeme (například Wireshark)

The Dude

Zobrazení struktury sítě

- volně šiřitelný software od MikroTiku pro Windows, přes Wine i v Linuxu
- zobrazuje seznam a mapu všech zařízení v síti, která jsou dostupná, monitoruje běžící služby, u některých zařízení i vzdálená správa

Struktura sítě



Nmap

- nmap (Network Mapper) je původem unixový program pro sledování stavu, služeb a prostředků sítě
- Zenmap je GUI frontend pro nmap
- dnes je nmap i pro Windows
- http://nmap.org/

- `nmap názevPC`
  - skenování spuštěných služeb (můžeme zadat i název našeho počítače)
- `nmap -sS -O názevPC`
  - (nutná vyšší oprávnění) aktivní skenování portů, zjištění informací o OS

Nessus

- software pro aktivní skenování zranitelností systému
- velmi užitečný pro administrátory – ověření bezpečnostního stavu sítě
- pro různé operační systémy, komerční i volná varianta (omezení na 16 IP adres)
- http://www.tenable.com/products/nessus

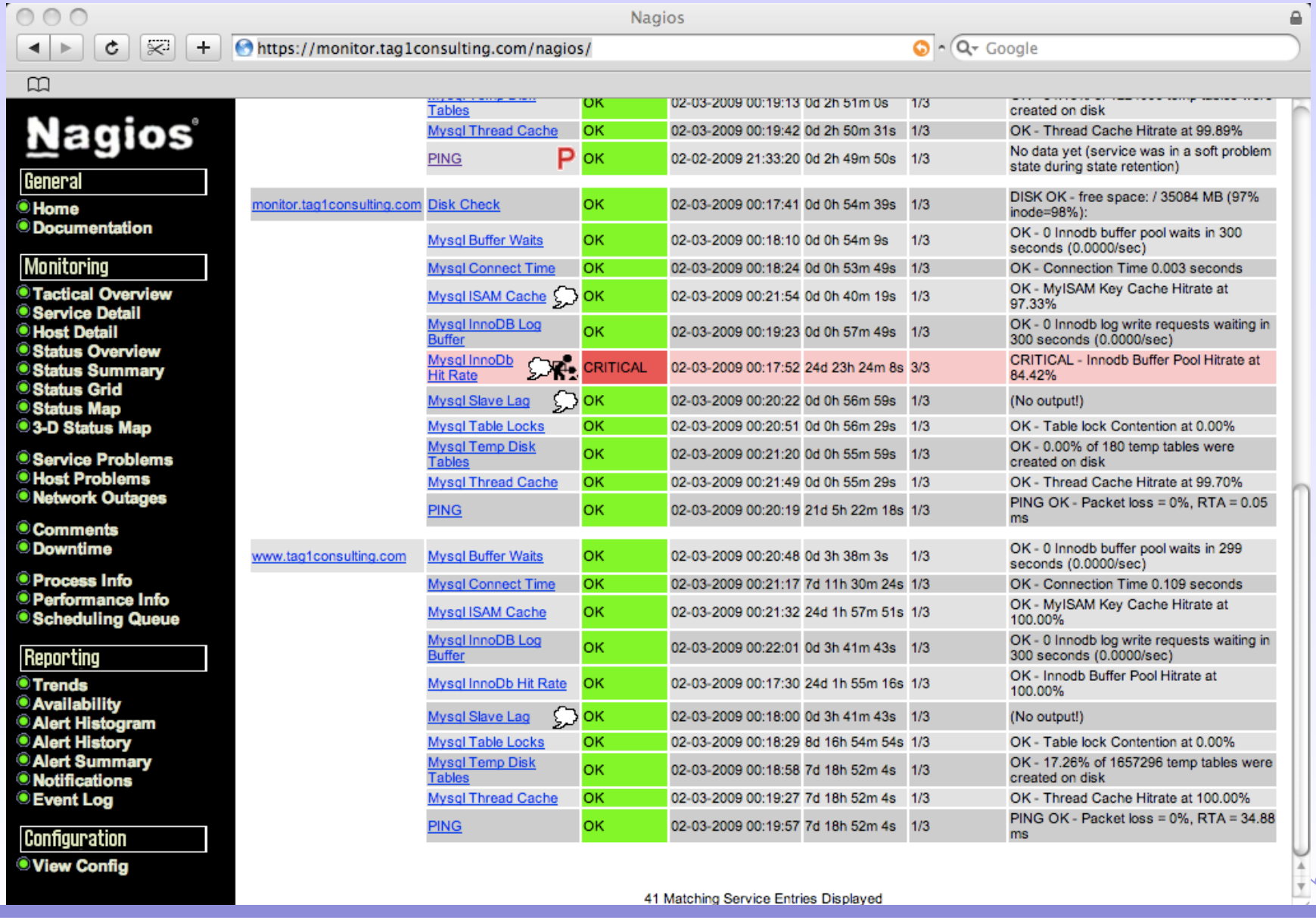
Struktura sítě

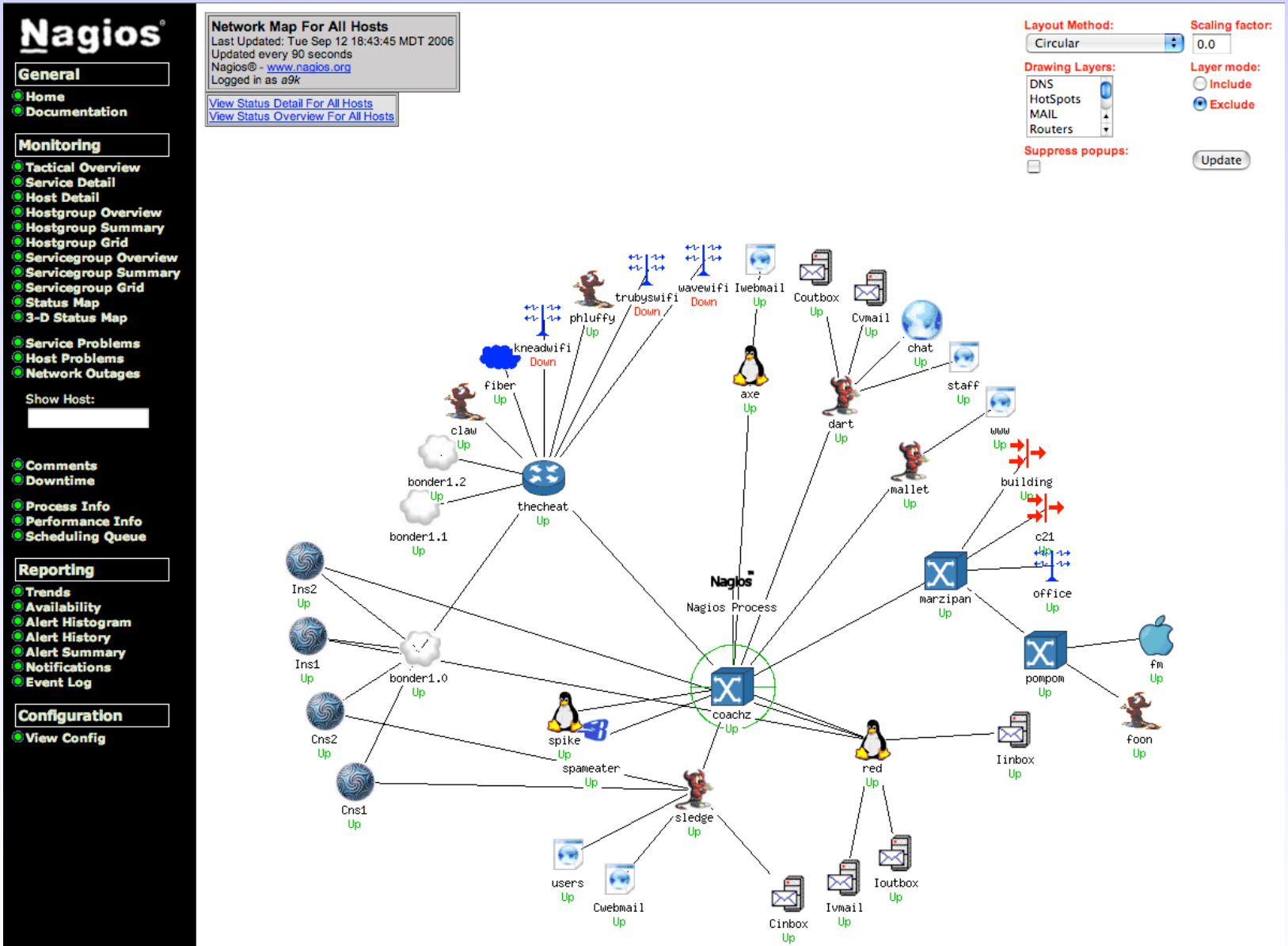
Co je to dohledový systém (network management software)

- je pokročilejší systém, který monitoruje stav sítě, sbírá informace z různých uzlů sítě, generuje reporty, v případě potřeby vhodně reaguje
- existuje hodně open-source dohledových systémů (Nagios, Zabbix, OpenNMS, Zenoss, Cacti, atd.
- je napojen na některou databázi, kterou naplňuje vhodný monitorovací systém (např. Snort)

Nagios

- monitoruje různé síťové služby (protokoly HTTP, SMTP, ICMP, atd.) včetně šifrovaných, využívání prostředků na uzlech sítě (Windows/Linux/Unix), umí vizualizovat stav sítě, apod.
- konfigurace přes webové rozhraní
- reakce v případě problémů:
  - okamžitý report (e-mail, SMS, pager, VoIP)
  - proaktivní ochrana (některé záchranné operace je schopen provést automaticky sám)


Nagios
https://monitor.tag1consulting.com/nagios/
Google
Nagios
General
Home
Documentation
Monitoring
Tactical Overview
Service Detail
Host Detail
Status Overview
Status Summary
Status Grid
Status Map
3-D Status Map
Service Problems
Host Problems
Network Outages
Comments
Downtime
Process Info
Performance Info
Scheduling Queue
Reporting
Trends
Availability
Alert Histogram
Alert History
Alert Summary
Notifications
Event Log
Configuration
View Config
Tables OK 02-03-2009 00:19:13 0d 2h 51m 0s 1/3 created on disk
Mysql Thread Cache OK 02-03-2009 00:19:42 0d 2h 50m 31s 1/3 OK - Thread Cache Hitrate at 99.89%
PING OK 02-02-2009 21:33:20 0d 2h 49m 50s 1/3 No data yet (service was in a soft problem state during state retention)
monitor.tag1consulting.com Disk Check OK 02-03-2009 00:17:41 0d 0h 54m 39s 1/3 DISK OK - free space: / 35084 MB (97% inode=98%):
Mysql Buffer Waits OK 02-03-2009 00:18:10 0d 0h 54m 9s 1/3 OK - 0 Innodb buffer pool waits in 300 seconds (0.0000/sec)
Mysql Connect Time OK 02-03-2009 00:18:24 0d 0h 53m 49s 1/3 OK - Connection Time 0.003 seconds
Mysql ISAM Cache OK 02-03-2009 00:21:54 0d 0h 40m 19s 1/3 OK - MyISAM Key Cache Hitrate at 97.33%
Mysql InnoDB Log Buffer OK 02-03-2009 00:19:23 0d 0h 57m 49s 1/3 OK - 0 Innodb log write requests waiting in 300 seconds (0.0000/sec)
Mysql InnoDb Hit Rate CRITICAL 02-03-2009 00:17:52 24d 23h 24m 8s 3/3 CRITICAL - Innodb Buffer Pool Hitrate at 84.42%
Mysql Slave Lag OK 02-03-2009 00:20:22 0d 0h 56m 59s 1/3 (No output!)
Mysql Table Locks OK 02-03-2009 00:20:51 0d 0h 56m 29s 1/3 OK - Table lock Contention at 0.00%
Mysql Temp Disk Tables OK 02-03-2009 00:21:20 0d 0h 55m 59s 1/3 OK - 0.00% of 180 temp tables were created on disk
Mysql Thread Cache OK 02-03-2009 00:21:49 0d 0h 55m 29s 1/3 OK - Thread Cache Hitrate at 99.70%
PING OK 02-03-2009 00:20:19 21d 5h 22m 18s 1/3 PING OK - Packet loss = 0%, RTA = 0.05 ms
www.tag1consulting.com Mysql Buffer Waits OK 02-03-2009 00:20:48 0d 3h 38m 3s 1/3 OK - 0 Innodb buffer pool waits in 299 seconds (0.0000/sec)
Mysql Connect Time OK 02-03-2009 00:21:17 7d 11h 30m 24s 1/3 OK - Connection Time 0.109 seconds
Mysql ISAM Cache OK 02-03-2009 00:21:32 24d 1h 57m 51s 1/3 OK - MyISAM Key Cache Hitrate at 100.00%
Mysql InnoDB Log Buffer OK 02-03-2009 00:22:01 0d 3h 41m 43s 1/3 OK - 0 Innodb log write requests waiting in 300 seconds (0.0000/sec)
Mysql InnoDb Hit Rate OK 02-03-2009 00:17:30 24d 1h 55m 16s 1/3 OK - Innodb Buffer Pool Hitrate at 100.00%
Mysql Slave Lag OK 02-03-2009 00:18:00 0d 3h 41m 43s 1/3 (No output!)
Mysql Table Locks OK 02-03-2009 00:18:29 8d 16h 54m 54s 1/3 OK - Table lock Contention at 0.00%
Mysql Temp Disk Tables OK 02-03-2009 00:18:58 7d 18h 52m 4s 1/3 OK - 17.26% of 1657296 temp tables were created on disk
Mysql Thread Cache OK 02-03-2009 00:19:27 7d 18h 52m 4s 1/3 OK - Thread Cache Hitrate at 100.00%
PING OK 02-03-2009 00:19:57 7d 18h 52m 4s 1/3 PING OK - Packet loss = 0%, RTA = 34.88 ms
41 Matching Service Entries Displayed


Nagios
General
Home
Documentation
Monitoring
Tactical Overview
Service Detail
Host Detail
Hostgroup Overview
Hostgroup Summary
Hostgroup Grid
Servicegroup Overview
Servicegroup Summary
Servicegroup Grid
Status Map
3-D Status Map
Service Problems
Host Problems
Network Outages
Show Host:
Comments
Downtime
Process Info
Performance Info
Scheduling Queue
Reporting
Trends
Availability
Alert Histogram
Alert History
Alert Summary
Notifications
Event Log
Configuration
View Config
Network Map For All Hosts
Last Updated: Tue Sep 12 18:43:45 MDT 2006
Updated every 90 seconds
Nagios® - www.nagios.org
Logged in as a9k
View Status Detail For All Hosts
View Status Overview For All Hosts
Layout Method:
Circular
Scaling factor:
0.0
Drawing Layers:
DNS
HotSpots
MAIL
Routers
Layer mode:
Include
Exclude
Suppress popups:
Update
wavewifi Down
Iwebmail Up
trubyswifi Down
Coutbox Up
Cvmail Up
phluffy Up
chat Up
kneadwifi Down
axe Up
staff Up
fiber Up
dart Up
claw Up
www Up
bonder1.2 Up
mallet Up
building Up
thecheat Up
c21 Up
bonder1.1 Up
Ins2 Up
Nagios
Nagios Process
marzipan Up
office Up
Ins1 Up
bonder1.0 Up
pompom Up
fm Up
coachz Up
Cns2 Up
spike Up
foon Up
spameater Up
red Up
Iinbox Up
Cns1 Up
sledge Up
users Up
Cwebmail Up
Ioutbox Up
Ivmail Up
Cinbox Up

Další sledovací systémy

http://www.hw-group.com/software/pd_snmp_cz.html
(přehled dohledových systémů, hodně komerčních, pár volně šiřitelných, příp. některé komerční, ale s malým počtem sledovaných uzlů zdarma)

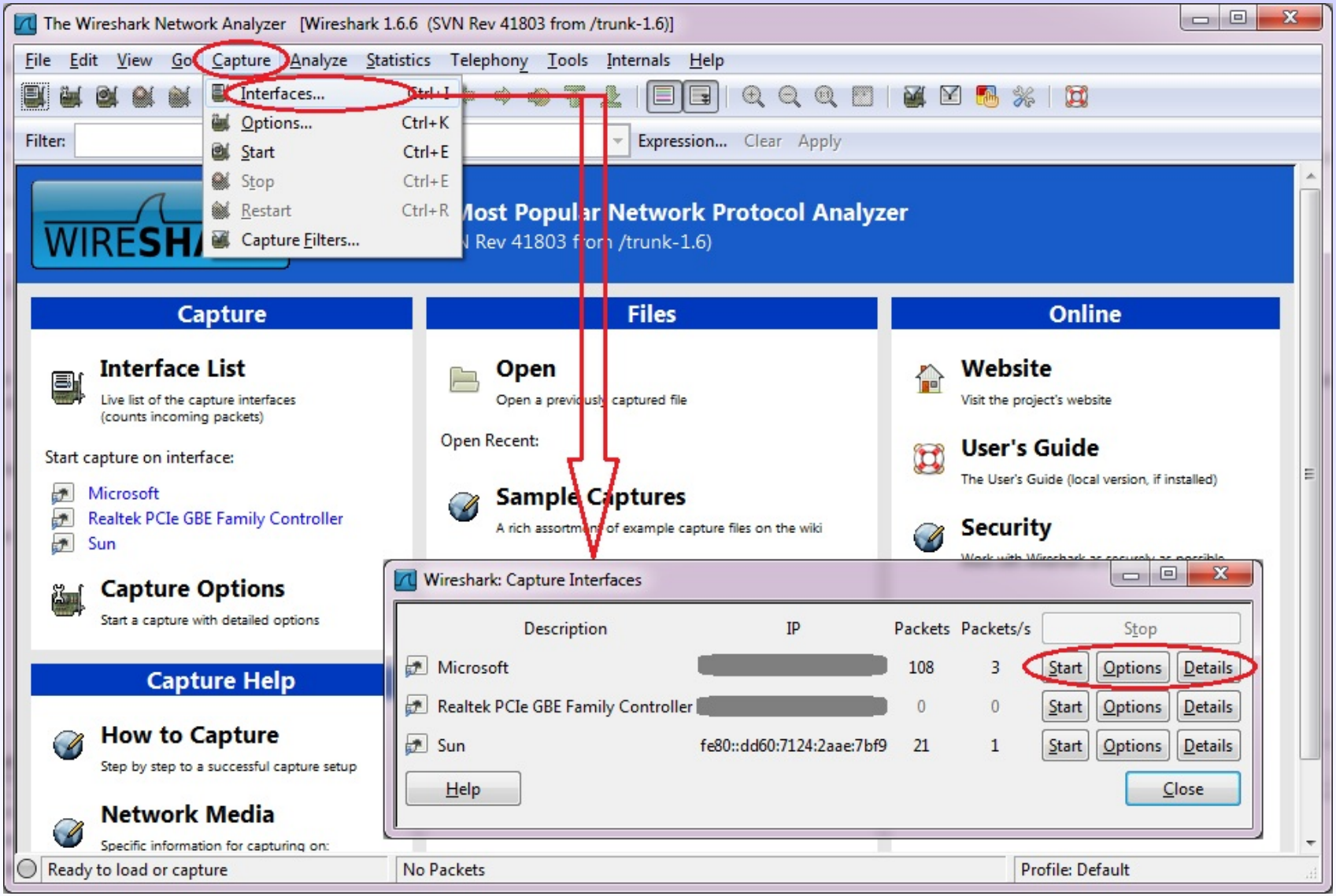
http://www.monitortools.com/

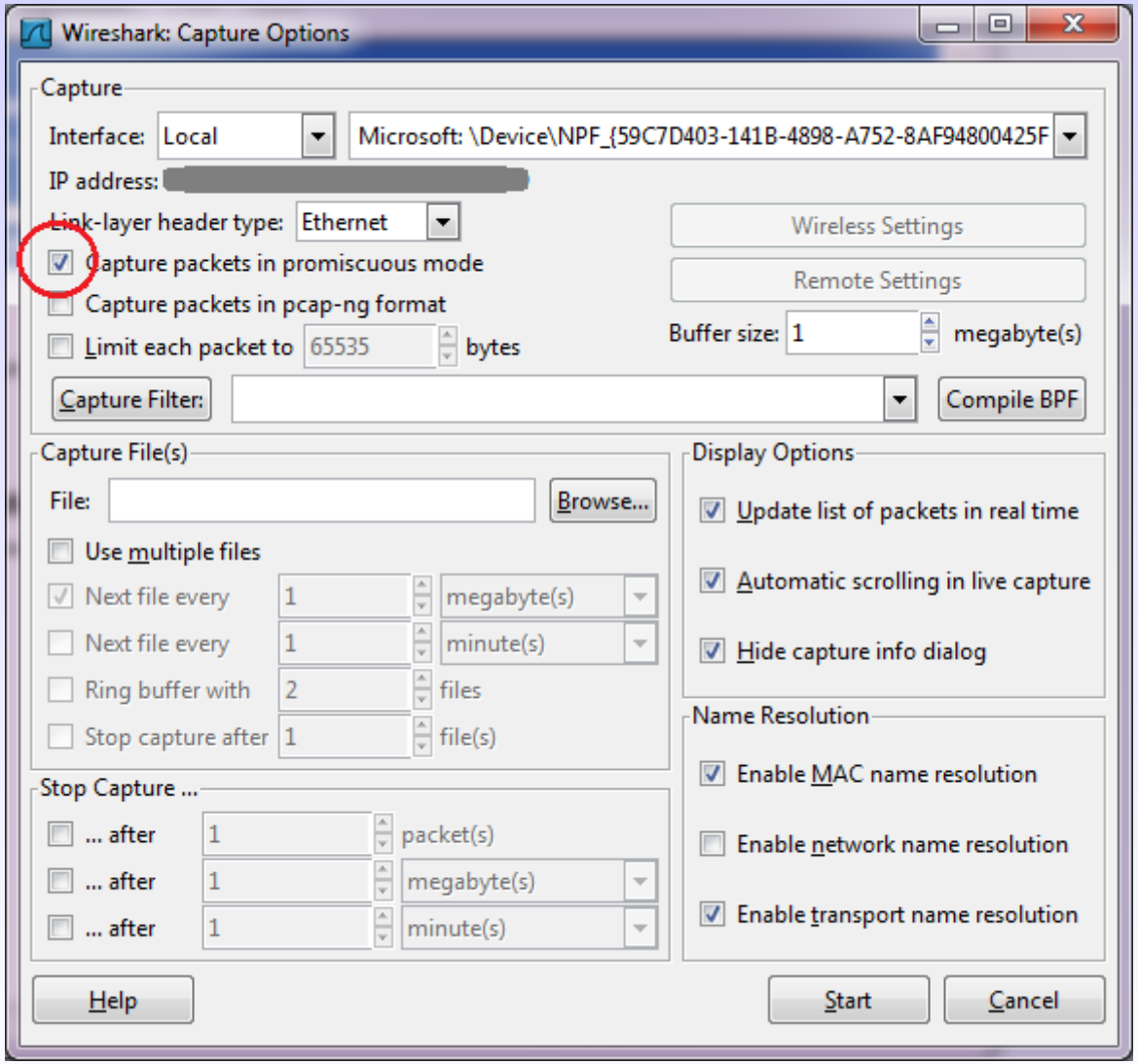
Packet sniffer

= program pro odposlech paketů v síti

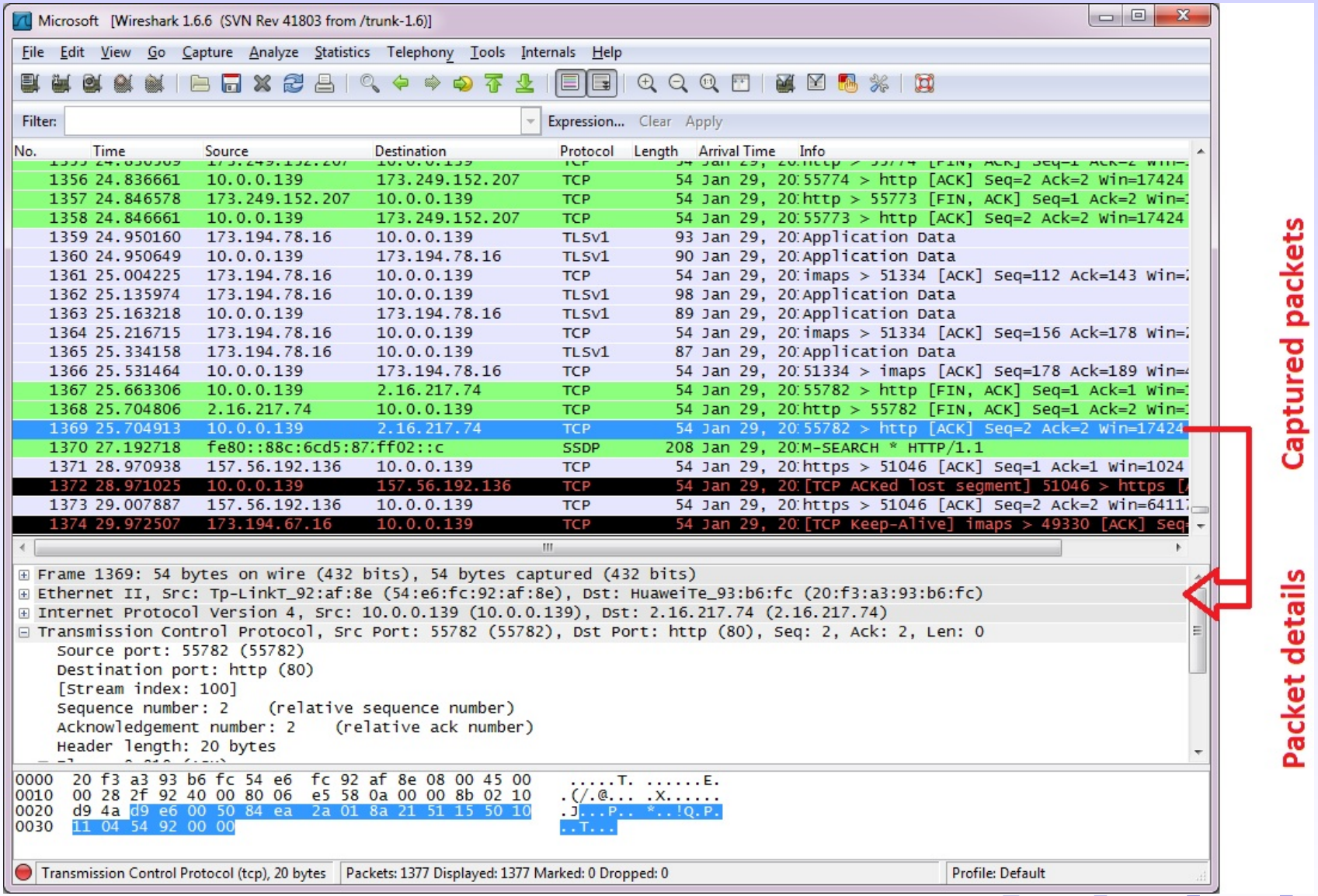
- získáme seznam zachycených paketů, ke každému veškeré informace (záhlaví/zápatí/data) z různých vrstev relačního modelu
- kdy použít: průzkum vlastní sítě, hledání problémů v konfiguraci síťových zařízení, hledání „závadné“ komunikace, apod.
- používané sniffery:
  - Wireshark http://www.wireshark.org/
  - tcpdump (je v Linuxu, příkazový režim)
  - Kismet(sniffer pro wi-fi sítě, spíše pro unixové systémy)
- další užitečné nástroje: http://sectools.org/

Packet sniffer




Wireshark: Capture Options
Capture
Interface: Local
Microsoft: \Device\NPF_{59C7D403-141B-4898-A752-8AF94800425F
IP address:
Link-layer header type: Ethernet
Capture packets in promiscuous mode
Capture packets in pcap-ng format
Limit each packet to 65535 bytes
Wireless Settings
Remote Settings
Buffer size: 1 megabyte(s)
Capture Filter:
Compile BPF
Capture File(s)
File:
Browse...
Use multiple files
Next file every 1 megabyte(s)
Next file every 1 minute(s)
Ring buffer with 2 files
Stop capture after 1 file(s)
Display Options
Update list of packets in real time
Automatic scrolling in live capture
Hide capture info dialog
Name Resolution
Enable MAC name resolution
Enable network name resolution
Enable transport name resolution
Stop Capture ...
... after 1 packet(s)
... after 1 megabyte(s)
... after 1 minute(s)
Help
Start
Cancel

Packet sniffer

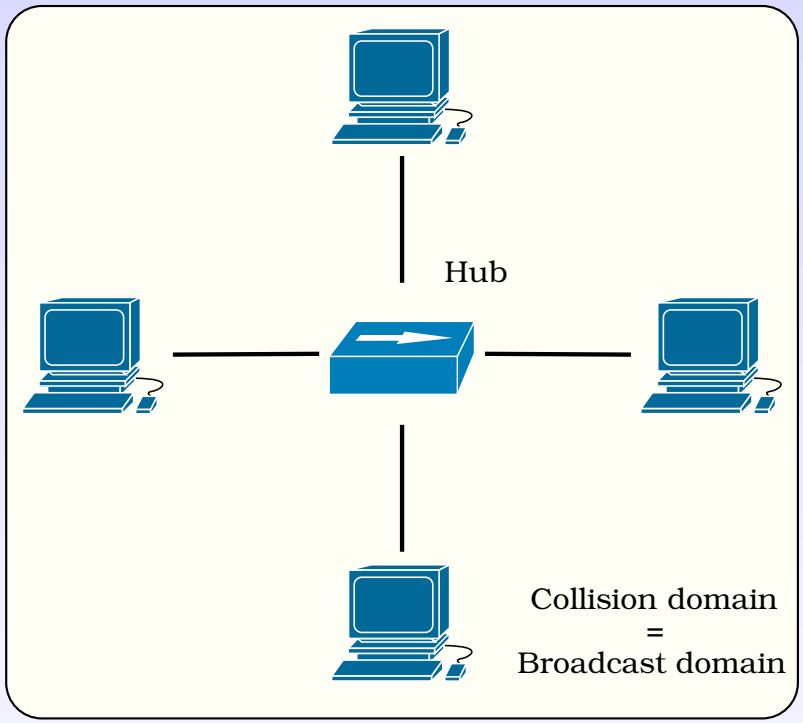


Kam se snifferem

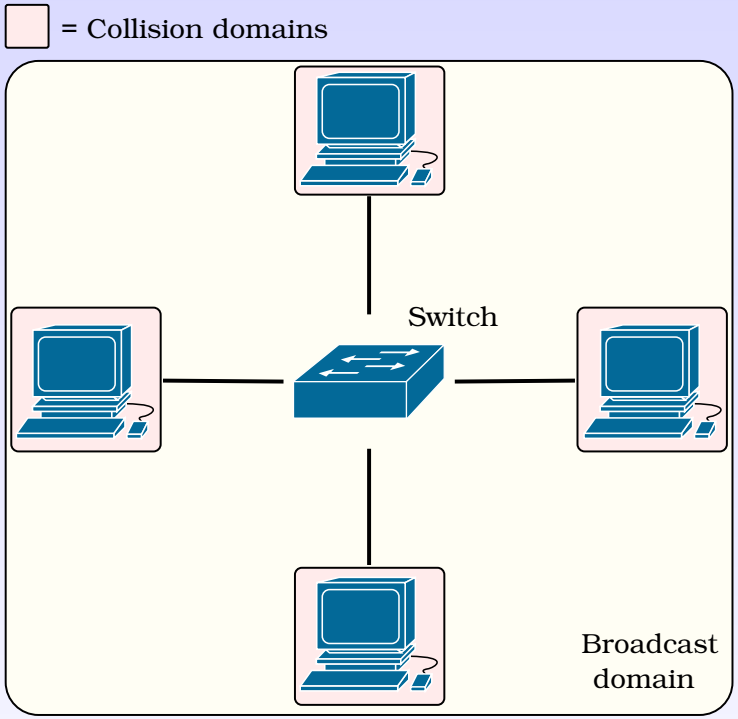
- hub (rozbočovač) neodděluje kolizní ani broadcast domény, ale hubů už moc není
- switch odděluje kolizní domény, neodděluje broadcast domény
  - když jsme připojeni ke switchi, odchytíme jen vlastní konverzaci a broadcasty
- router odděluje kolizní i broadcast domény
  - odchytíme jen vlastní konverzaci

Čím dál, tím hůř jsme schopni provoz hlídat a diagnostikovat.

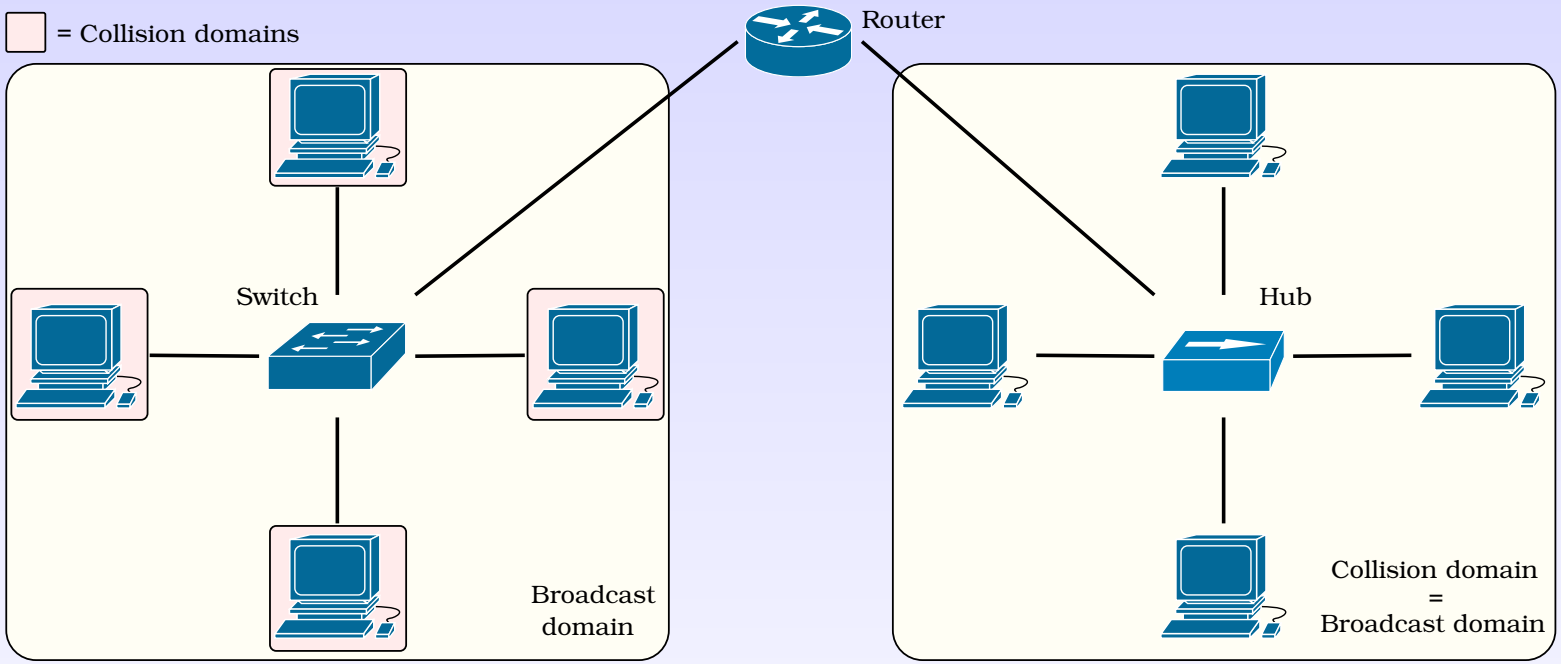
Hub



Switch

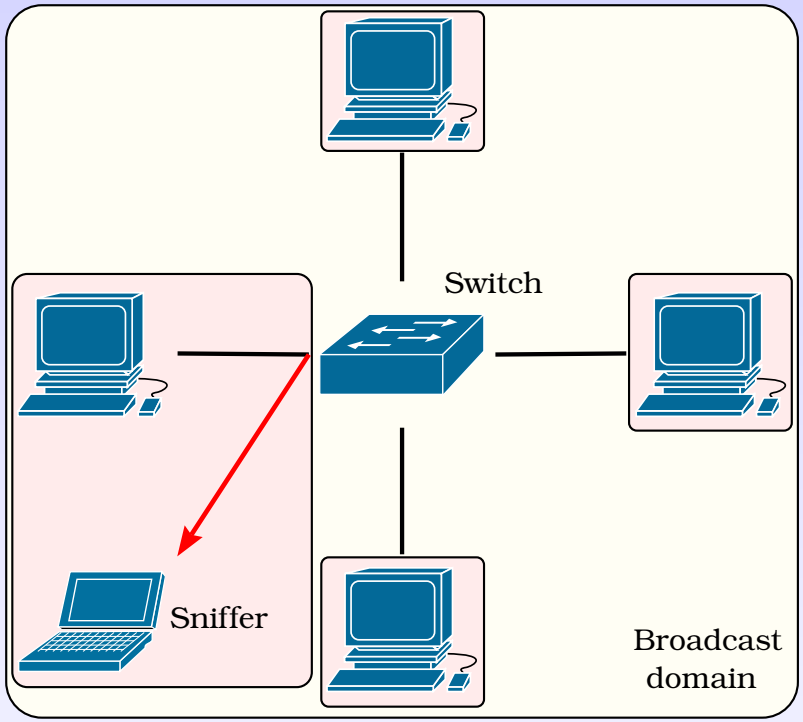


Router


= Collision domains
Router
Switch
Broadcast domain
Hub
Collision domain = Broadcast domain

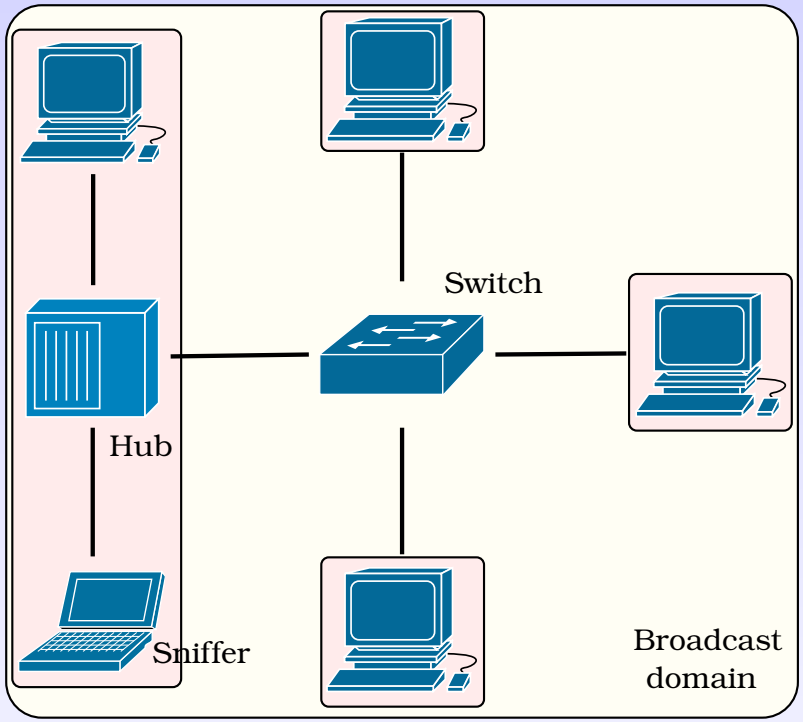
Možnosti řešení

- Zrcadlení portů (port mirroring, port spanning)
  - podporují dražší firemní switche
  - v konfiguraci stanovíme jeden port (pro sniffer), na který se bude zrcadlit provoz jiného portu


Switch
Sniffer
Broadcast
domain

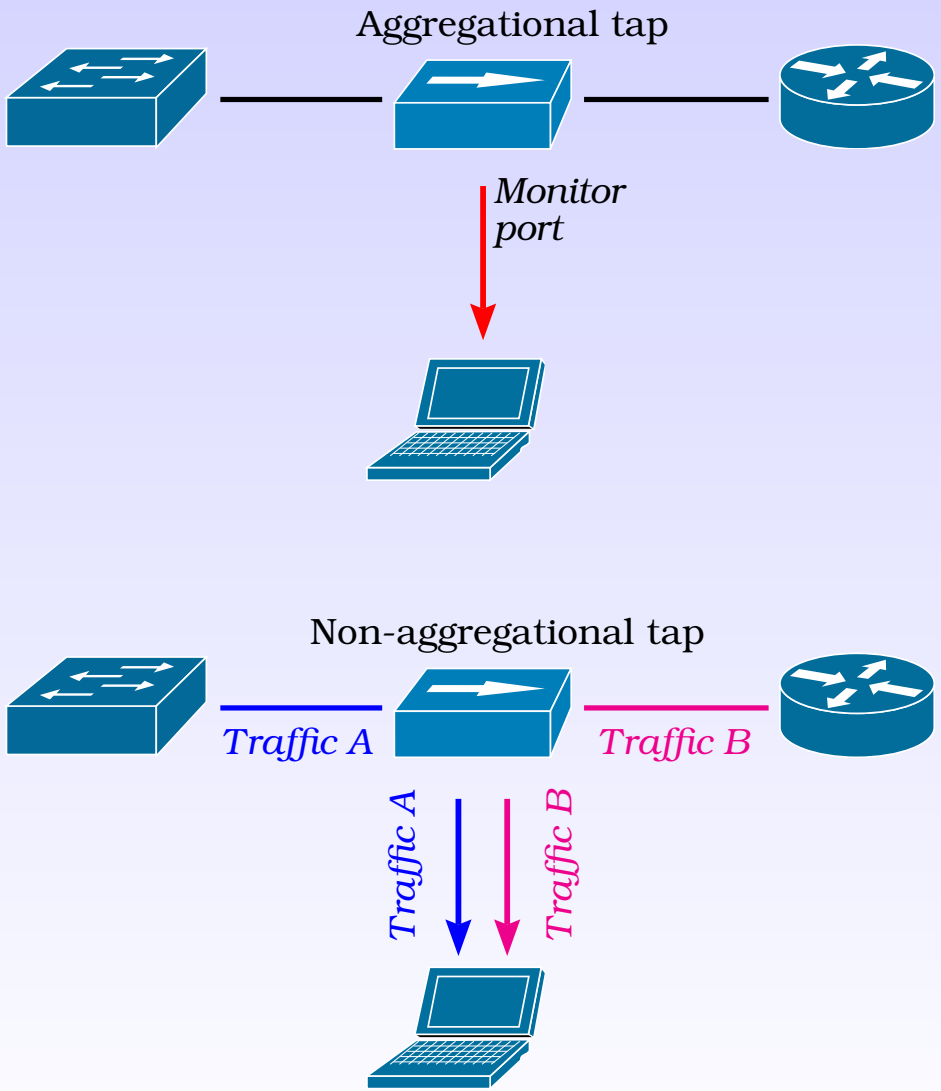
Možnosti řešení

- Zrcadlení portů (port mirroring, port spanning)
  - podporují dražší firemní switche
  - v konfiguraci stanovíme jeden port (pro sniffer), na který se bude zrcadlit provoz jiného portu
- použití rozbočovače (hubbing out)
  - k zrcadlení provozu použijeme hub, pokud se nám ho podaří sehnat


Switch
Hub
Sniffer
Broadcast
domain

Možnosti řešení

- Zrcadlení portů (port mirroring, port spanning)
  - podporují dražší firemní switche
  - v konfiguraci stanovíme jeden port (pro sniffer), na který se bude zrcadlit provoz jiného portu
- použití rozbočovače (hubbing out)
  - k zrcadlení provozu použijeme hub, pokud se nám ho podaří sehnat
- síťový odposlech (network tap)
  - podobně jako předchozí, ale jde o speciální síťový prvek


Aggregational tap
Monitor port
Non-aggregational tap
Traffic A
Traffic B
Traffic A
Traffic B