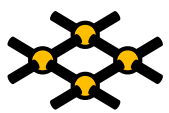
Záchyt paketů a protokoly

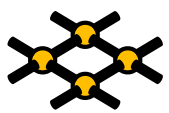
Petr Holub

PB156cv
2021–03–08



Cíle cvičení

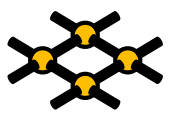
- Seznámit se základy síťového provozu
- Pochopit základy návrhu experimentů a tvorby protokolů.
- Vyzkoušet si prakticky tvorbu protokolu – dokumentovat a vyhodnotit experiment.



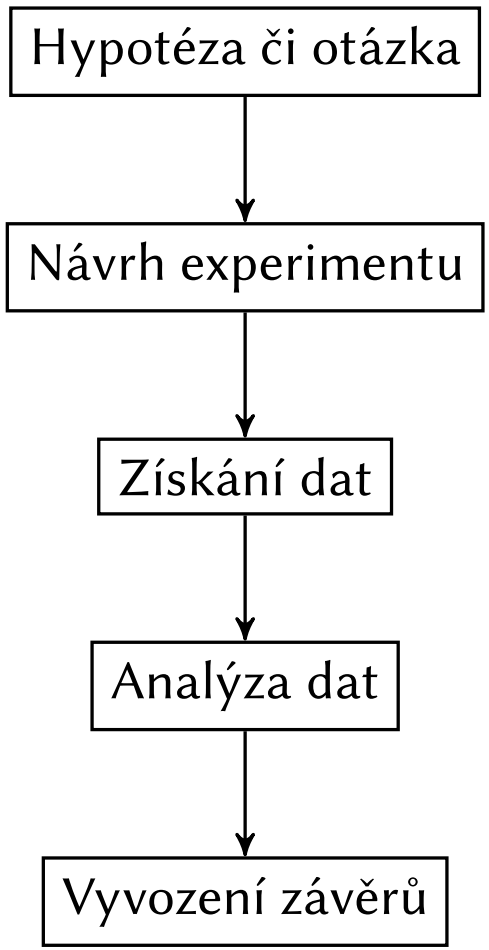
Experimenty a protokoly

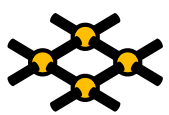
Základy experimentální práce

- **Proč informatik potřebuje experimenty?**
- Informatika má silné nástroje pro zjišťování faktů
  - důkazy
  - výpočty
  - simulace
- Praktické studium vlastností systémů
  - některé vlastnosti neumíme nebo z důvodu obtížnosti nemůžeme simulovat
- Podpoření nebo vyvrácení hypotézy
  - pozor… nedokazujeme!

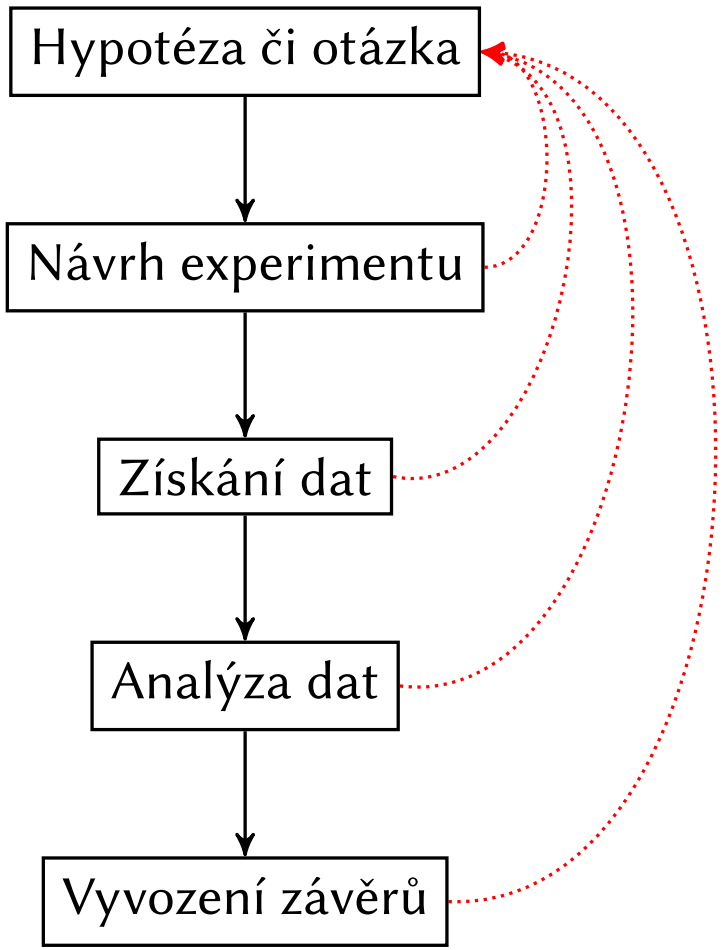


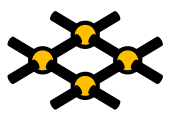
Co znamená provést experiment?





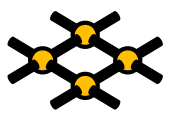
Co znamená provést experiment?





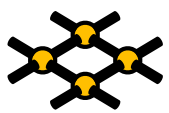
Proč protokoly?

- Potřebujeme zachytit informace o exprimentu až po vyvození závěrů.
  1. Jaká byla hypotéza či otázka?
  2. Co jsem dělal(a) a proč jsem to dělal(a)?
  3. Jaké jsou výsledky a jejich vyhodnocení?
  4. Jaké jsem vyvodil(a) závěry?
- Popis experimentu tak, aby bylo možné jej reprodukovat.
  - Někdy se rozlišuje mezi replikací (stejným člověkem ve stejné laboratoči) a reprodukcí experimentu (někým jiným někde jinde).



Co by měl protokol obsahovat?

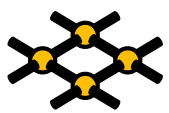
- **Vše co je nezbytné k reprodukování experimentu:**
  - písemná formulace hypotézy/otázky,
  - dokumentace návrhu experimentu,
  - dokumentace provedení experimentu vč. podmínek, které by mohly mít vliv na výsledky,
  - dokumentace analýzy dat,
  - vyvození závěrů.



Analýza síťového provozu

Nastavení počítače pro záchyt paketů

- Je vhodné minimalizovat vlastní provoz generovaný počítačem.
  - Vypnout demony typu Avahi
    `service avahi-daemon stop`
  - Nastavit statickou konfiguraci a vypnout automatické systémy (např. Network Manager na Linuxu)
    `service network-manager stop`
  - Vypnout IPv6
    `echo 1 >/proc/sys/net/ipv6/conf/enp0s31f6/disable_ipv6`
  - Odnastavit IPv4 adresy
    `ifconfig enp0s31f6 0`
    `ifconfig enp0s31f6 down`
    `ifconfig enp0s31f6 up`
- tcpdump
  `tcpdump -i eth0 -c 1000 -s 100 -w /tmp/file icmp`



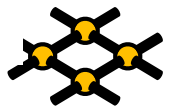
Wireshark

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	147.251.106.133	239.255.255.250	SSDP	366	NOTIFY * HTTP/1.1

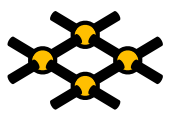
```
Frame 1: 366 bytes on wire (2928 bits), 366 bytes captured (2928 bits) on interface \Device\NPF_{196B5099-6092-4C36-8EBE-B78E7B230357}, id 0
Ethernet II, Src: JuniperN_e9:06:0b (f4:cc:55:e9:06:0b), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
    Destination: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
    Source: JuniperN_e9:06:0b (f4:cc:55:e9:06:0b)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 147.251.106.133, Dst: 239.255.255.250
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 352
    Identification: 0x0000 (0)
    Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 1
    Protocol: UDP (17)
    Header checksum: 0x8a12 [validation disabled]
    [Header checksum status: Unverified]
    Source: 147.251.106.133
    Destination: 239.255.255.250
User Datagram Protocol, Src Port: 1900, Dst Port: 1900
    Source Port: 1900
    Destination Port: 1900
    Length: 332
    Checksum: 0xdc71 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
    [Timestamps]
Simple Service Discovery Protocol
    NOTIFY * HTTP/1.1\r\n
    LOCATION: http://147.251.106.133:57549/\r\n
    HOST: 239.255.255.250:1900\r\n
    SERVER: POSIX, UPnP/1.0, Intel MicroStack/1.0.1868\r\n
    NTS: ssdp:alive\r\n
    USN: uuid:5e3cb924-542b-4877-a9f1-0013E208EB6C::urn:schemas-upnp-org:device:VideoServer:1\r\n
    CACHE-CONTROL: max-age=30\r\n
    NT: urn:schemas-upnp-org:device:VideoServer:1\r\n
    \r\n
    [Full request URI: http://239.255.255.250:1900*]
```



Wireshark

```
> Frame 1: 366 bytes on wire (2928 bits), 366 bytes captured (2928 bits) on interface \Device\NPF_{196B5099-6092
v Ethernet II, Src: JuniperN_e9:06:0b (f4:cc:55:e9:06:0b), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
  > Destination: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
  > Source: JuniperN_e9:06:0b (f4:cc:55:e9:06:0b)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 147.251.106.133, Dst: 239.255.255.250
> User Datagram Protocol, Src Port: 1900, Dst Port: 1900
v Simple Service Discovery Protocol
  > NOTIFY * HTTP/1.1\r\n
    LOCATION: http://147.251.106.133:57549/\r\n
    HOST: 239.255.255.250:1900\r\n
    SERVER: POSIX, UPnP/1.0, Intel MicroStack/1.0.1868\r\n
    NTS: ssdp:alive\r\n
    USN: uuid:5e3cb924-542b-4877-a9f1-0013E208EB6C::urn:schemas-upnp-org:device:VideoServer:1\r\n
    CACHE-CONTROL: max-age=30\r\n
    NT: urn:schemas-upnp-org:device:VideoServer:1\r\n
    \r\n
    [Full request URI: http://239.255.255.250:1900*]
```

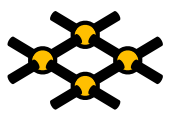
```
0000  01 00 5e 7f ff fa f4 cc  55 e9 06 0b 08 00 45 00   ..^..... U.....E.
0010  01 60 00 00 40 00 01 11  8a 12 93 fb 6a 85 ef ff   .`..@... ....j...
0020  ff fa 07 6c 07 6c 01 4c  dc 71 4e 4f 54 49 46 59   ...l.l.L .qNOTIFY
0030  20 2a 20 48 54 54 50 2f  31 2e 31 0d 0a 4c 4f 43    * HTTP/ 1.1..LOC
0040  41 54 49 4f 4e 3a 20 68  74 74 70 3a 2f 2f 31 34   ATION: h ttp://14
```



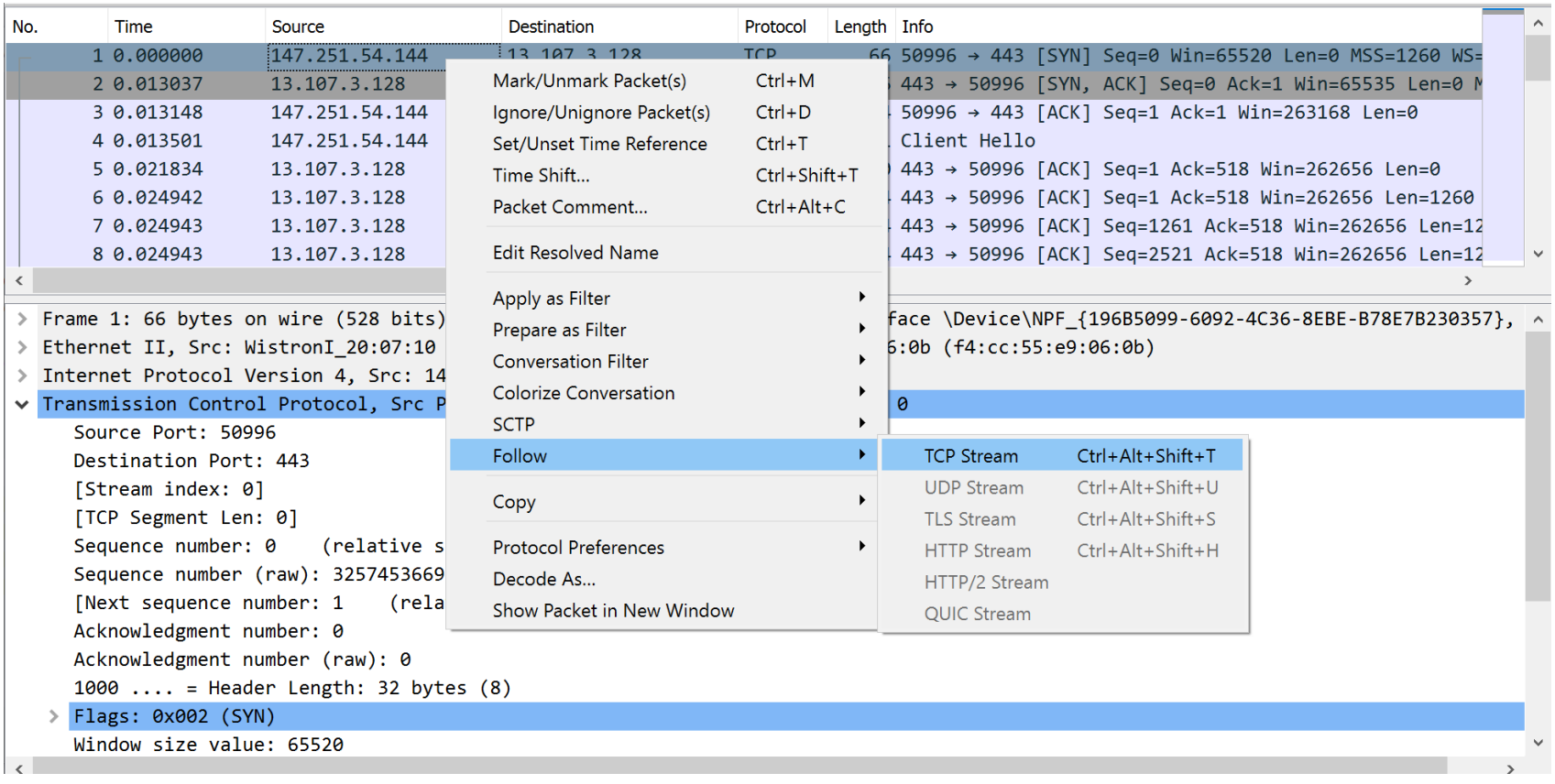
Wireshark

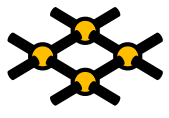
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	147.251.54.144	13.107.3.128	TCP	66	50996 → 443 [SYN] Seq=0 Win=65520 Len=0 MSS=1260 WS=
2	0.013037	13.107.3.128	147.251.54.144	TCP	66	443 → 50996 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 M
3	0.013148	147.251.54.144	13.107.3.128	TCP	54	50996 → 443 [ACK] Seq=1 Ack=1 Win=263168 Len=0
4	0.013501	147.251.54.144	13.107.3.128	TLSv1.2	571	Client Hello
5	0.021834	13.107.3.128	147.251.54.144	TCP	60	443 → 50996 [ACK] Seq=1 Ack=518 Win=262656 Len=0
6	0.024942	13.107.3.128	147.251.54.144	TCP	1314	443 → 50996 [ACK] Seq=1 Ack=518 Win=262656 Len=1260
7	0.024943	13.107.3.128	147.251.54.144	TCP	1314	443 → 50996 [ACK] Seq=1261 Ack=518 Win=262656 Len=12
8	0.024943	13.107.3.128	147.251.54.144	TCP	1314	443 → 50996 [ACK] Seq=2521 Ack=518 Win=262656 Len=12

```
> Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{196B5099-6092-4C36-8EBE-B78E7B230357},
> Ethernet II, Src: WistronI_20:07:10 (48:2a:e3:20:07:10), Dst: JuniperN_e9:06:0b (f4:cc:55:e9:06:0b)
> Internet Protocol Version 4, Src: 147.251.54.144, Dst: 13.107.3.128
v Transmission Control Protocol, Src Port: 50996, Dst Port: 443, Seq: 0, Len: 0
    Source Port: 50996
    Destination Port: 443
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    Sequence number (raw): 3257453669
    [Next sequence number: 1    (relative sequence number)]
    Acknowledgment number: 0
    Acknowledgment number (raw): 0
    1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x002 (SYN)
    Window size value: 65520
```

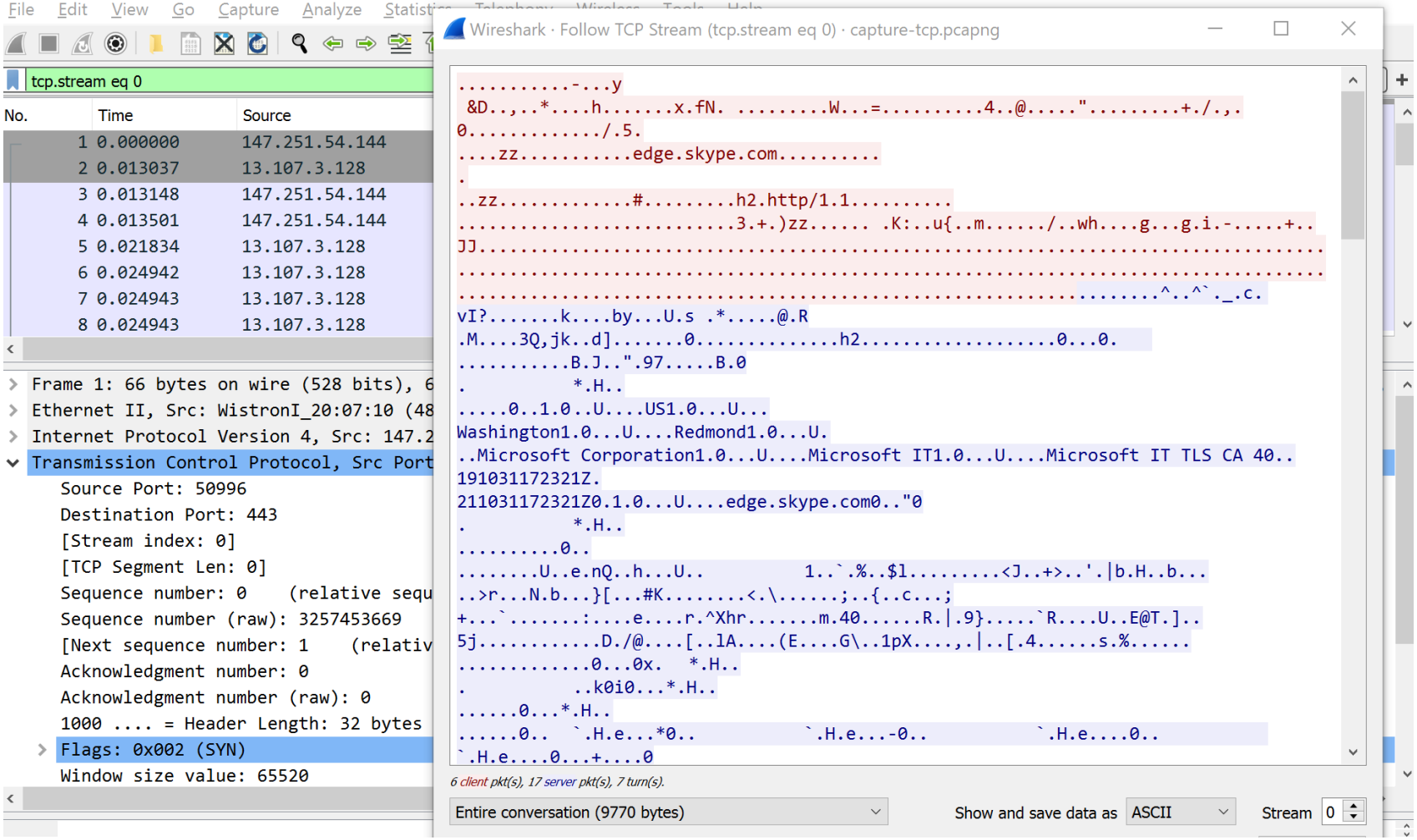


Wireshark


No. Time Source Destination Protocol Length Info
1 0.000000 147.251.54.144 13.107.3.128 TCP 66 50996 → 443 [SYN] Seq=0 Win=65520 Len=0 MSS=1260 WS=
2 0.013037 13.107.3.128 443 → 50996 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 M
3 0.013148 147.251.54.144 50996 → 443 [ACK] Seq=1 Ack=1 Win=263168 Len=0
4 0.013501 147.251.54.144 Client Hello
5 0.021834 13.107.3.128 443 → 50996 [ACK] Seq=1 Ack=518 Win=262656 Len=0
6 0.024942 13.107.3.128 443 → 50996 [ACK] Seq=1 Ack=518 Win=262656 Len=1260
7 0.024943 13.107.3.128 443 → 50996 [ACK] Seq=1261 Ack=518 Win=262656 Len=12
8 0.024943 13.107.3.128 443 → 50996 [ACK] Seq=2521 Ack=518 Win=262656 Len=12
Frame 1: 66 bytes on wire (528 bits)
Ethernet II, Src: WistronI_20:07:10
Internet Protocol Version 4, Src: 14
Transmission Control Protocol, Src P
Source Port: 50996
Destination Port: 443
[Stream index: 0]
[TCP Segment Len: 0]
Sequence number: 0 (relative s
Sequence number (raw): 3257453669
[Next sequence number: 1 (rela
Acknowledgment number: 0
Acknowledgment number (raw): 0
1000 .... = Header Length: 32 bytes (8)
Flags: 0x002 (SYN)
Window size value: 65520
face \Device\NPF_{196B5099-6092-4C36-8EBE-B78E7B230357},
6:0b (f4:cc:55:e9:06:0b)
0
Mark/Unmark Packet(s) Ctrl+M
Ignore/Unignore Packet(s) Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift... Ctrl+Shift+T
Packet Comment... Ctrl+Alt+C
Edit Resolved Name
Apply as Filter
Prepare as Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
Copy
Protocol Preferences
Decode As...
Show Packet in New Window
TCP Stream Ctrl+Alt+Shift+T
UDP Stream Ctrl+Alt+Shift+U
TLS Stream Ctrl+Alt+Shift+S
HTTP Stream Ctrl+Alt+Shift+H
HTTP/2 Stream
QUIC Stream

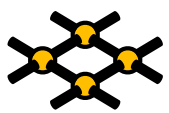


Wireshark


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.stream eq 0
No. Time Source
1 0.000000 147.251.54.144
2 0.013037 13.107.3.128
3 0.013148 147.251.54.144
4 0.013501 147.251.54.144
5 0.021834 13.107.3.128
6 0.024942 13.107.3.128
7 0.024943 13.107.3.128
8 0.024943 13.107.3.128
Frame 1: 66 bytes on wire (528 bits), 6
Ethernet II, Src: WistronI_20:07:10 (48
Internet Protocol Version 4, Src: 147.2
Transmission Control Protocol, Src Port
Source Port: 50996
Destination Port: 443
[Stream index: 0]
[TCP Segment Len: 0]
Sequence number: 0 (relative sequ
Sequence number (raw): 3257453669
[Next sequence number: 1 (relativ
Acknowledgment number: 0
Acknowledgment number (raw): 0
1000 .... = Header Length: 32 bytes
Flags: 0x002 (SYN)
Window size value: 65520
Wireshark · Follow TCP Stream (tcp.stream eq 0) · capture-tcp.pcapng
.....-...y
&D..,..*....h.....x.fN. .....W...=.....4..@....."....+./.,.
0...../.5.
....zz.....edge.skype.com.....
.
..zz.....#.....h2.http/1.1.....
.....3.+.)zz..... .K:..u{..m...../..wh...g...g.i.-.....+..
JJ.....
.....^..^`._.c.
vI?.....k....by...U.s .*.....@.R
.M....3Q,jk..d].....0.....h2.....0...0.
.....B.J..".97.....B.0
. *.H..
.....0..1.0..U....US1.0...U...
Washington1.0...U....Redmond1.0...U.
..Microsoft Corporation1.0...U....Microsoft IT1.0...U....Microsoft IT TLS CA 40..
1910311723212.
21103117232120.1.0...U....edge.skype.com0.."0
. *.H..
.....0..
.....U..e.nQ..h...U.. 1..`.%..$1.....<J..+>..'.|b.H..b...
..>r...N.b...}[...#K.....<.\.....;..{..c...;
+...`.....:....e....r.^Xhr.....m.40.....R.|.9}.....`R....U..E@T.]..
5j.....D./@....[..lA....(E....G\..1pX...,.|..[.4.....s.%.....
.....0...0x. *.H..
. ..k0i0...*.H..
.....0...*.H..
.....0.. `.H.e...*0.. `.H.e...-0.. `.H.e....0..
`.H.e....0...+....0
6 client pkt(s), 17 server pkt(s), 7 turn(s).
Entire conversation (9770 bytes)
Show and save data as ASCII
Stream 0

Zadání

- Vzvedněte si z Učebních materiálů PCAP soubor (`cviceni01`)
  - soubory jsou individuální a různé
- Zanalyzujte zachycené pakety
  - charakterizujte typy provozu, které v síti vidíte
  - proveďte co nejpodrobnější analýzu hlaviček 3 paketů z různých toků
- Zachyťte pomocí WireShark-u nebo tcpdump-u cca 200 paketů z vlastní sítě
  - charakterizujte typy provozu, které v síti vidíte

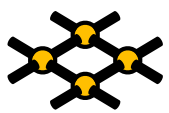


Protokol

Každý samostatně zpracuje a odevzdá protokol. Protokol musí obsahovat minimálně následující části:

- charakterizaci typů provozu z dodaného PCAP souboru
- podrobná analýza hlaviček 3 paketů z různých toků z dodaného PCAP souboru
- charakterizaci typů provozu ve vámi zachycených paketech
- PCAP soubor s výstupem vlastního zachytávání paketů

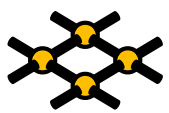
Protokol bude zpracován pomocí šablony v IS MU – `scanform.tar.bz2`
Experiment i protokol zpracuje **každý sám!**



Příprava na další cvičení

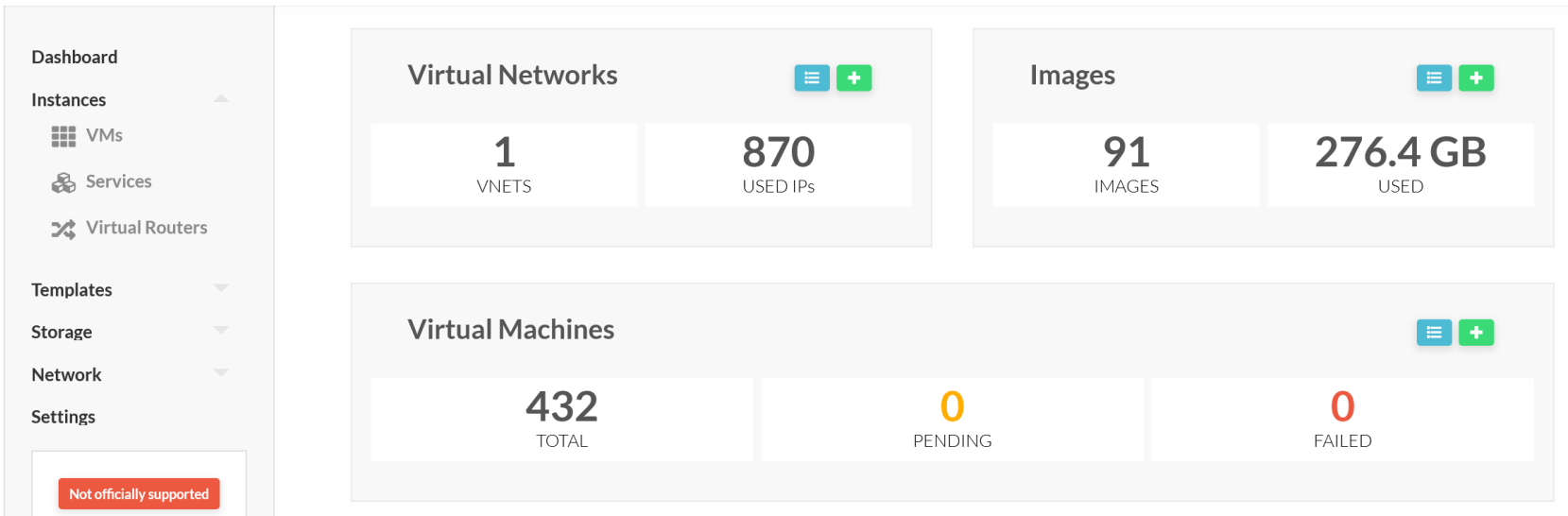
Práce s virtuálními stroji

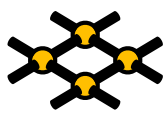
- Každý bude mít přiřazené 2 virtuální stroje
- Správa přes `https://stratus.fi.muni.cz/`
  - přihlášení přes fakultní login/heslo
  - možnost startu/restartu stroje, připojení přes VNC konzolu v prohlížeči
  - root heslo `unixfi_provided`
  - stroje se automaticky restartují to výchozího nastavení mezi 23:00 a 02:00



Práce s virtuálními stroji

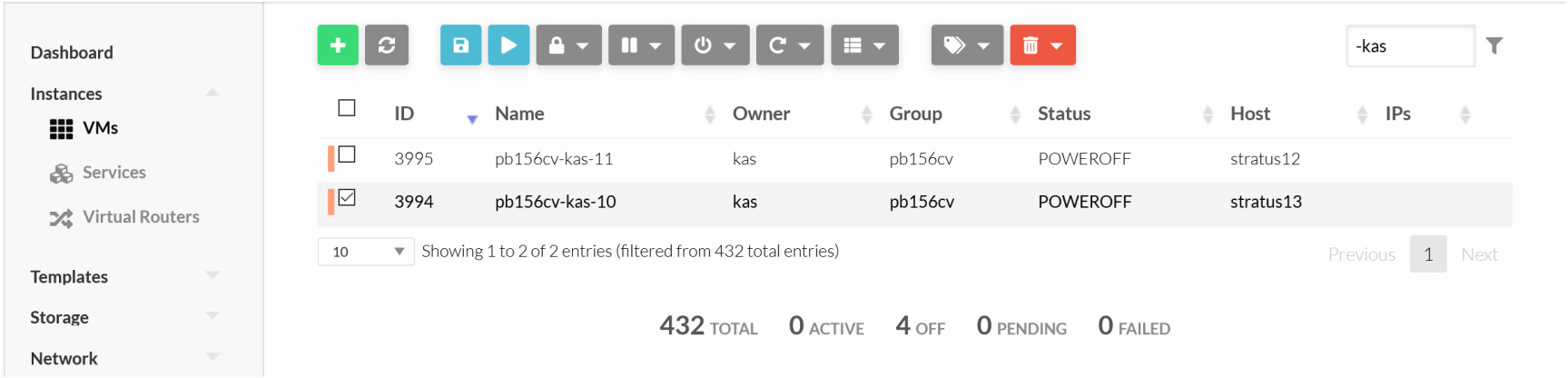
- Každý bude mít přiřazené 2 virtuální stroje
- Správa přes `https://stratus.fi.muni.cz/`

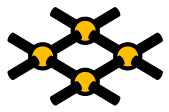




Práce s virtuálními stroji

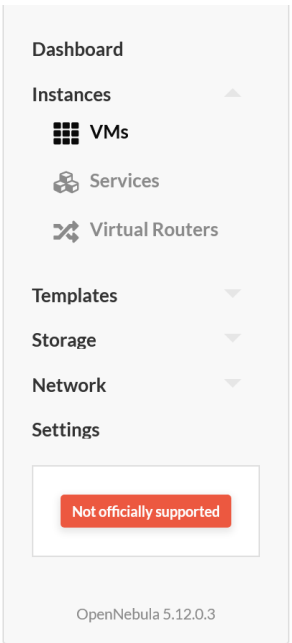
- Každý bude mít přiřazené 2 virtuální stroje
- Správa přes `https://stratus.fi.muni.cz/`

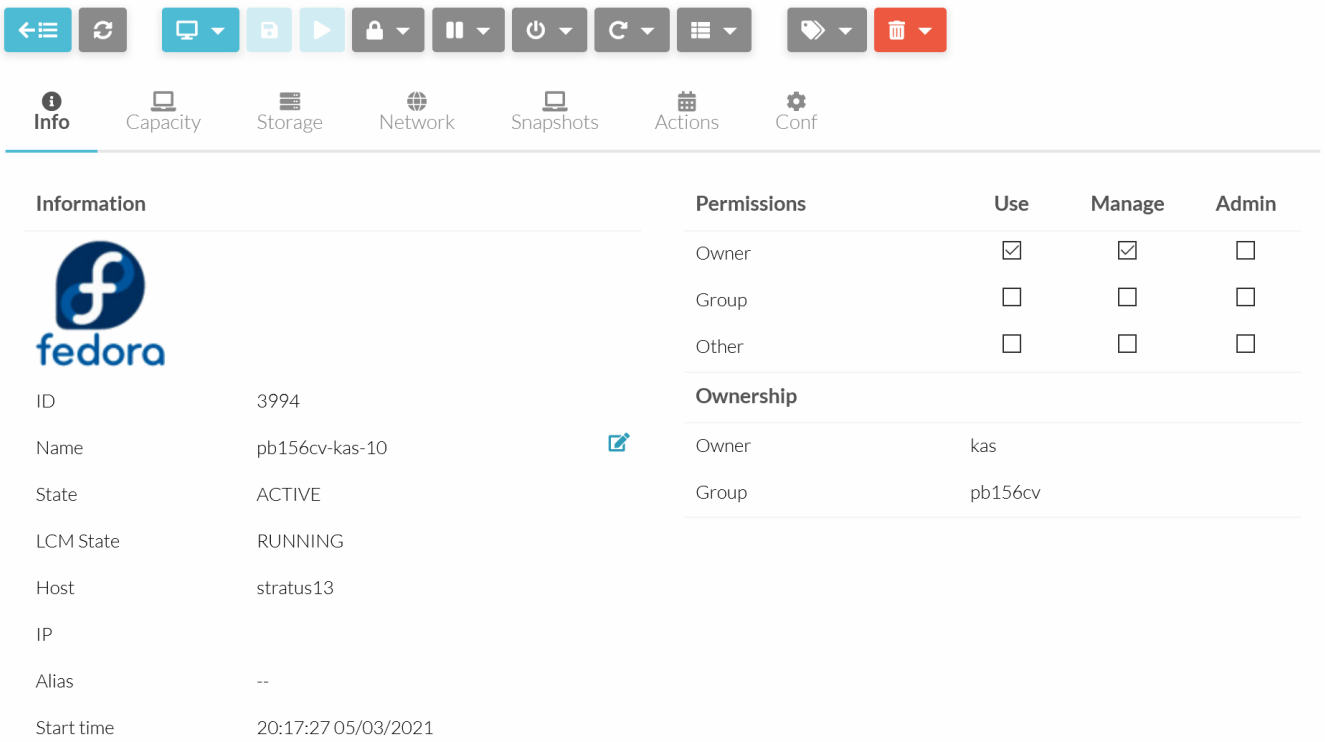


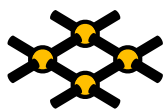


Práce s virtuálními stroji

- Každý bude mít přiřazené 2 virtuální stroje
- Správa přes `https://stratus.fi.muni.cz/`

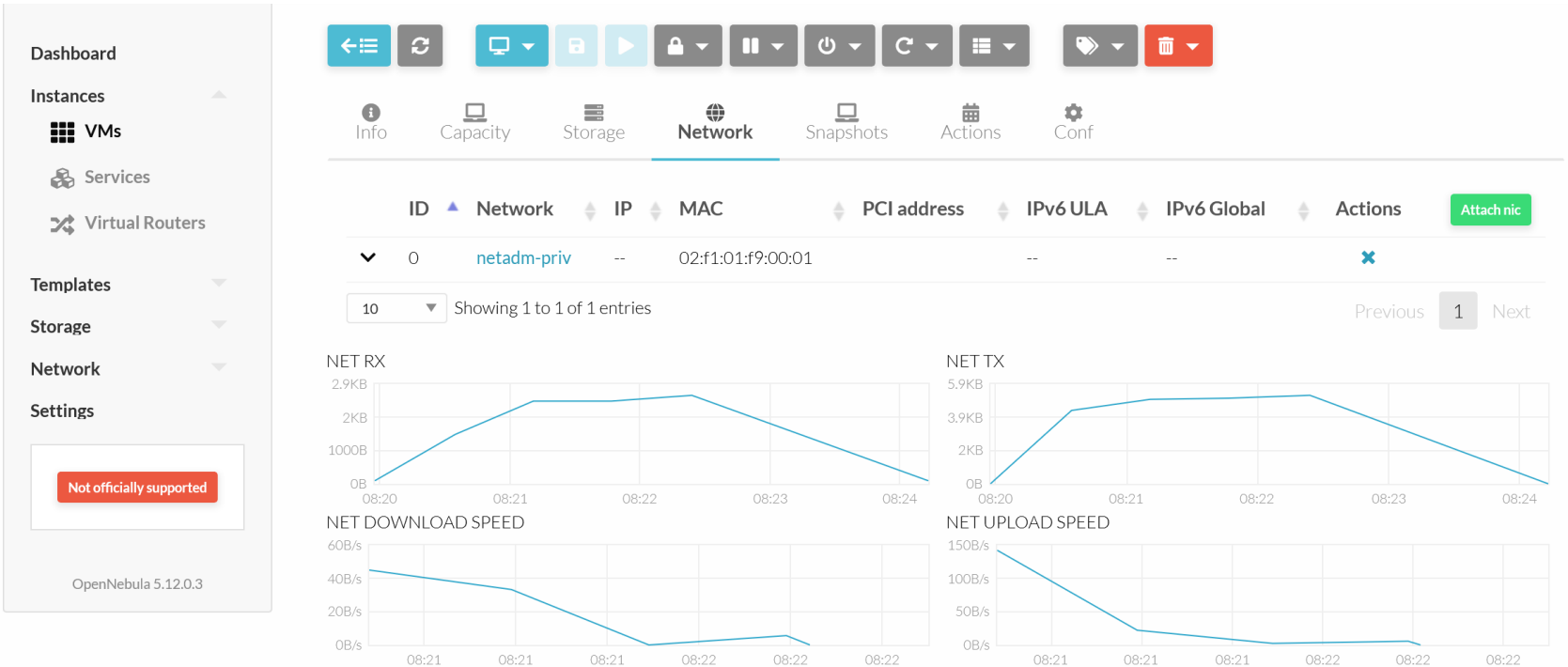






Práce s virtuálními stroji

- Každý bude mít přiřazené 2 virtuální stroje
- Správa přes `https://stratus.fi.muni.cz/`



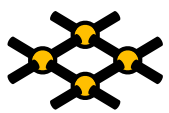
Práce s virtuálními stroji

- Gateway `ssh netadm-gw.fi.muni.cz`
  - potřeba být v univerzitní síti – VPN `https://it.muni.cz/sluzby/vpn`
  - přihlášení přes fakultní login/heslo
  - dohledání VM podle ARP

```
$ ssh xholub2@netadm-gw.fi.muni.cz
xholub2@netadm-gw.fi.muni.cz's password:
|
| Hosted at Stratus.fi.muni.cz. Cloud platform provided by unix@fi.mu
|
Last login: Sat Mar  6 09:36:07 2021 from 147.251.55.142

[xholub2@netadm-gw ~]$ arp -a | fgrep 02:f1:01:f9:00:01
? (10.0.1.10) at 02:f1:01:f9:00:01 [ether] on eth1
[xholub2@netadm-gw ~]$
```

Doplňující informace

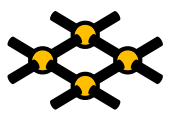


Literatura I

Zdeněk Horák.
Praktická fysika.
Státní nakladatelství technické literatury, Praha, 1958.

František Šťastný.
Zpracování experimentálních dat.
Katedra obecné fyziky PřF MU, Brno, 1997.
http://amper.ped.muni.cz/jenik/nejistoty/frst_zed.pdf.

Milan Meloun and Jiří Militký.
Data analysis in the chemical laboratory part 1. analysis of indirect measurements.
Analytica Chimica Acta, 293(1-2):183–189, 1994.
http://www.sciencedirect.com/science/article/B6TF4-44HT11Y-6D/2/eb0dc71f565eaf9211806cb31425a66a.



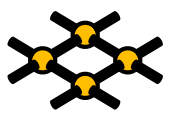
Literatura II

Patrick L. Brockett.
On the misuse of the central limit theorem in some risk calculations.
The Journal of Risk and Insurance, 50(4):727–731, December 1983.
http://www.jstor.org/stable/pdfplus/252712.pdf.

Jason W. Osborne.
Normalizing data transformations. ERIC digest.
Technical report, ERIC Clearinghouse on Assessment and Evaluation College Park MD, August 2002.
http://www.ericdigests.org/2003-3/data.htm.

George E. P. Box, J. Stuart Hunter, and William G. Hunter.
Statistics for Experimenters: Design, Innovation, and Discovery.
Wiley-Interscience, second edition, May 2005.

C. F. Jeff Wu and Michael Hamada.
Experiments: Planning, Analysis, and Parameter Design Optimization.
Wiley-Interscience, April 2000.



Literatura III


William G. Cochran and Gertrude M. Cox.
Experimental Designs.
Wiley, second edition, April 1992.