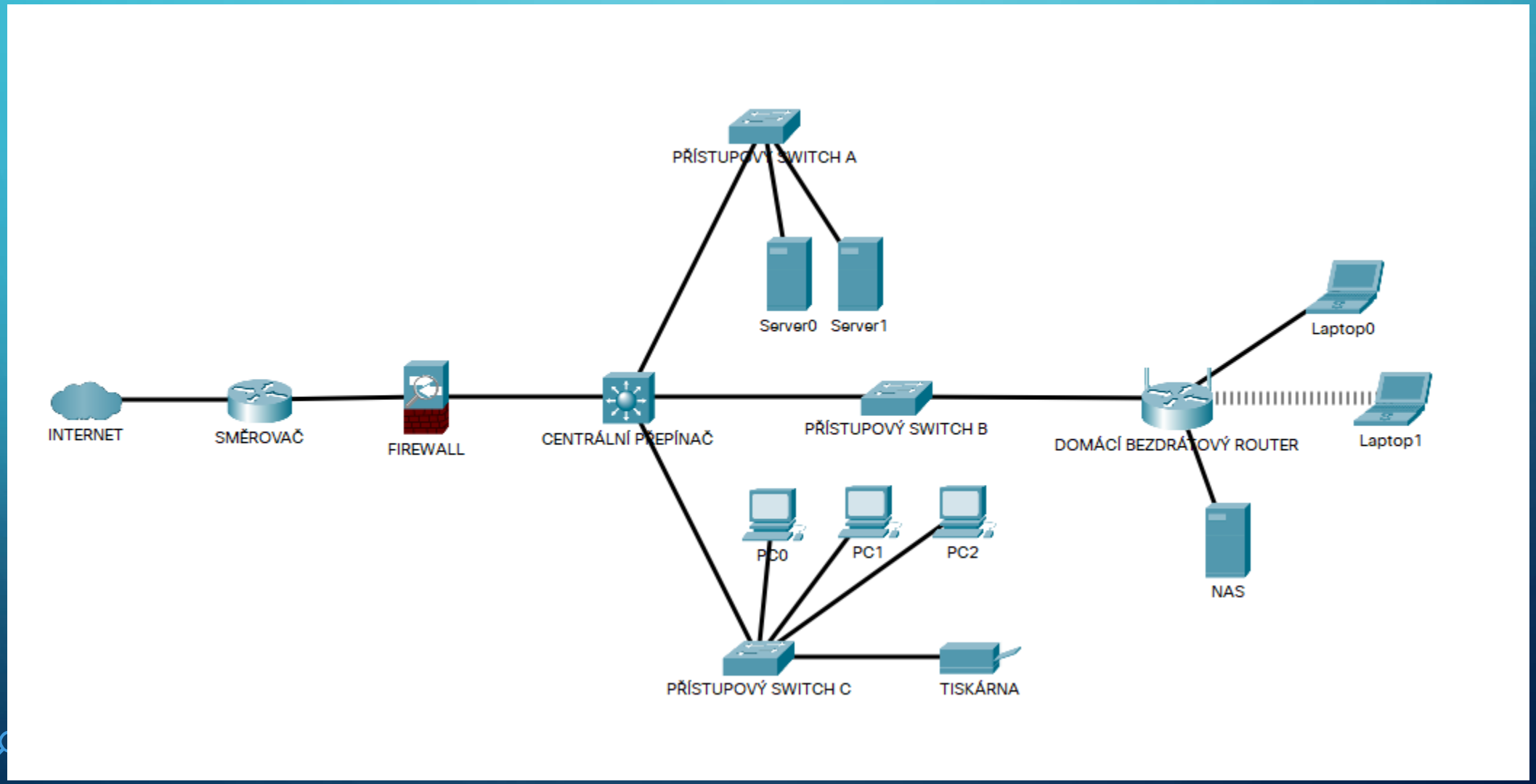
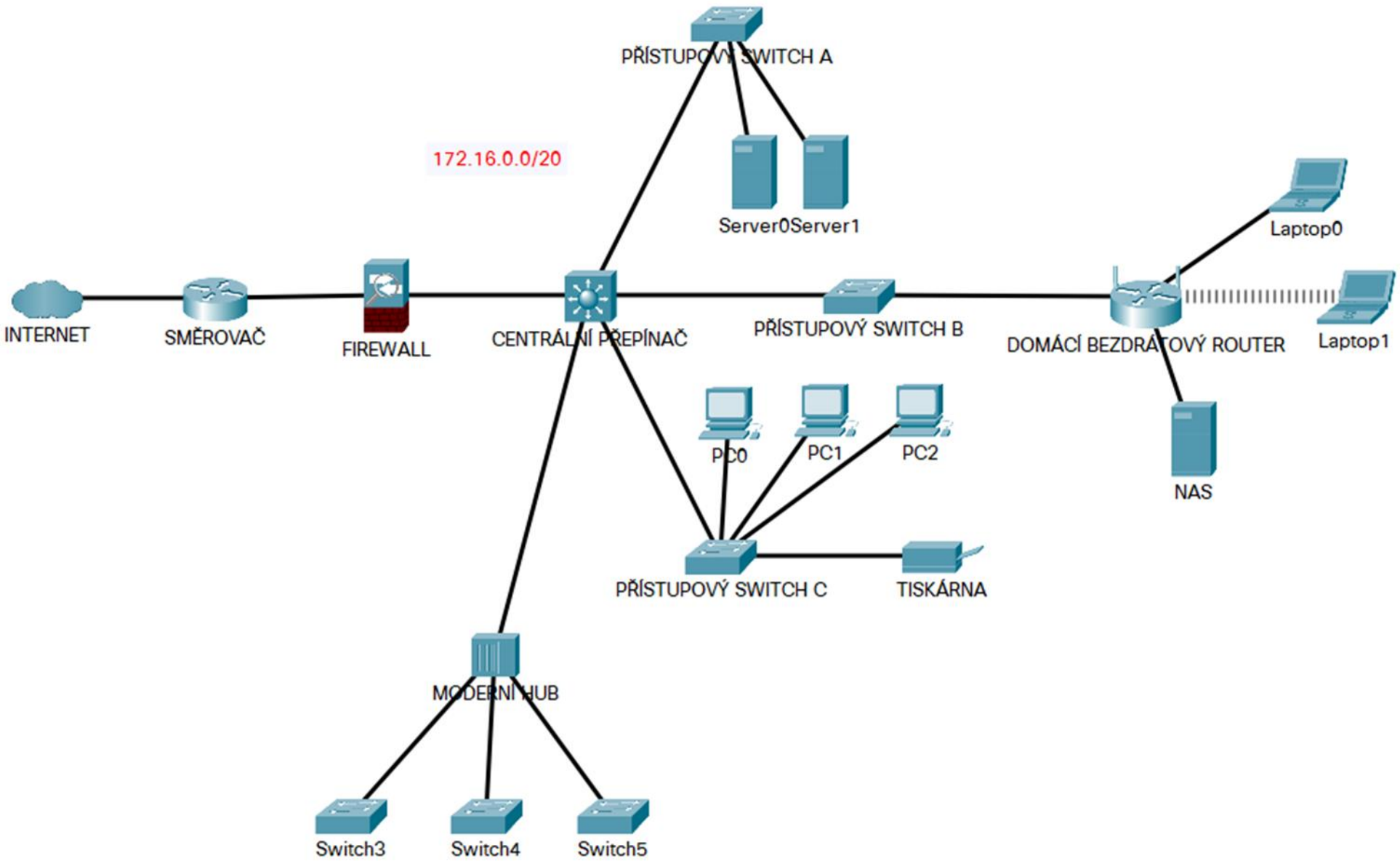
MOHLO BY TO TAKTO VYPADAT?

JAROMÍR HOLEC

ADMINISTRACE ÚSTAVNÍCH SÍTÍ




PŘÍSTUPOVÝ SWITCH A
172.16.0.0/20
Server0Server1
Laptop0
INTERNET
SMĚROVAČ
FIREWALL
CENTRÁLNÍ PŘEPÍNAČ
PŘÍSTUPOVÝ SWITCH B
DOMÁCÍ BEZDRÁTOVÝ ROUTER
Laptop1
PC0
PC1
PC2
NAS
PŘÍSTUPOVÝ SWITCH C
TISKÁRNA
MODERNÍ HUB
Switch3
Switch4
Switch5

ADMINISTRACE ÚSTAVNÍCH SÍTÍ – CO SE V SÍTI DĚJE?

- 23.12.2034 – 15:35 – POŽADAVEK NA PORUŠENÍ AUTORSKÝCH PRÁV
- 23.12.2034 – 17:35 – KOMUNIKACE S C&C BOTNETU
  - DST IP 18.214.21.235
- 30.12.2034 – 08:35 – PODIVNÉ CHOVÁNÍ SÍŤOVÉ INFRASTRUKTURY

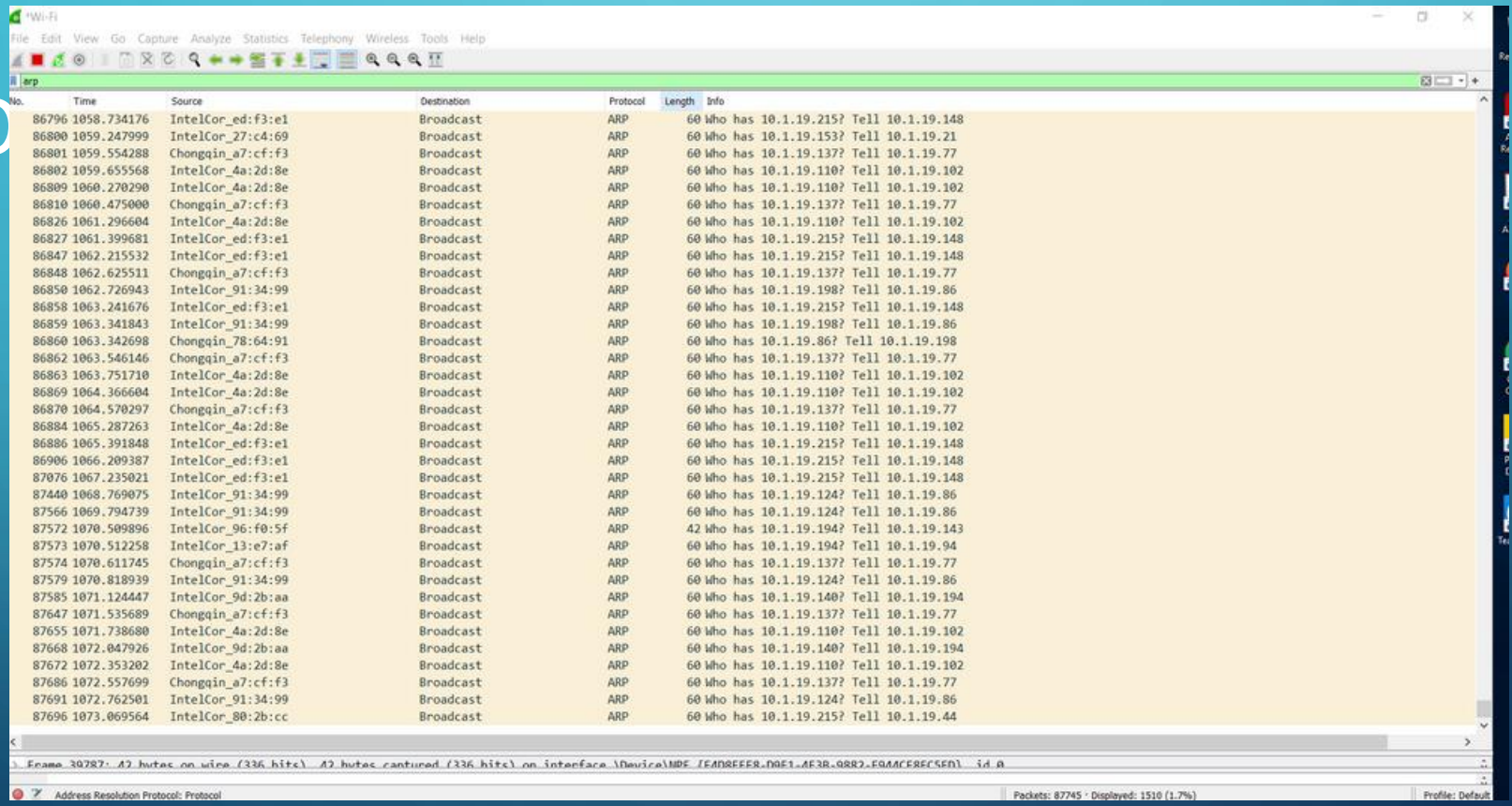
ADMINISTRACE ÚSTAVNÍCH SÍTÍ – CO SE V SÍTI DĚJE?

- NASAZENÍ MONITORINGU AKTIVNÍCH SÍTOVÝCH PRVKŮ
  - ZABBIX
  - ICINGA
  - NAGIOS
  - SOLARWINDS

ADMINISTRACE ÚSTAVNÍCH SÍTÍ – MONITORINGU AKTIVNÍCH SÍTOVÝCH PRVKŮ

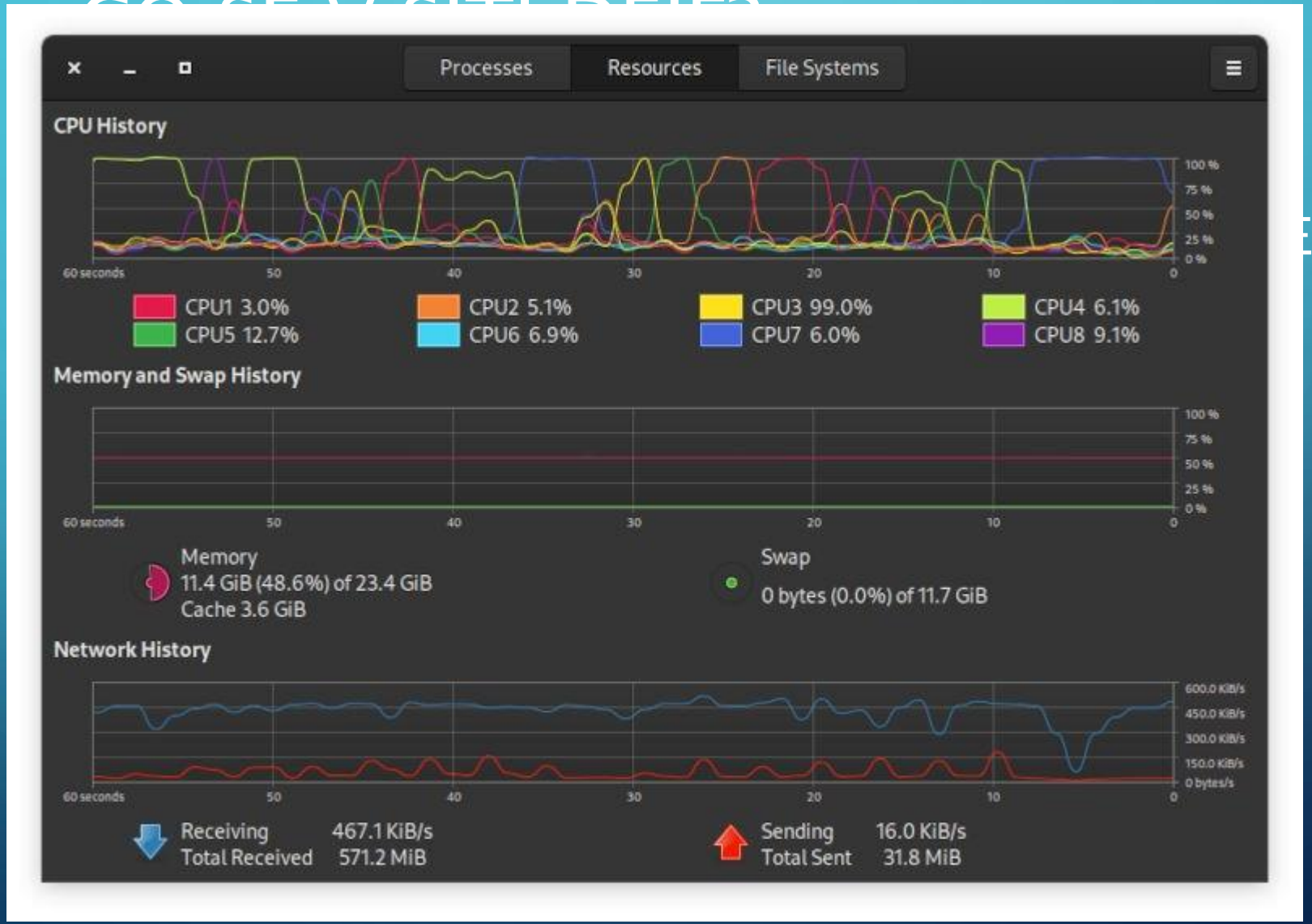
ADMINISTRACE ÚSTAVNÍCH SÍTÍ – CO SE V SÍTI DĚJE?

POD RY



ADMINISTRACE ÚSTAVNÍCH SÍTÍ

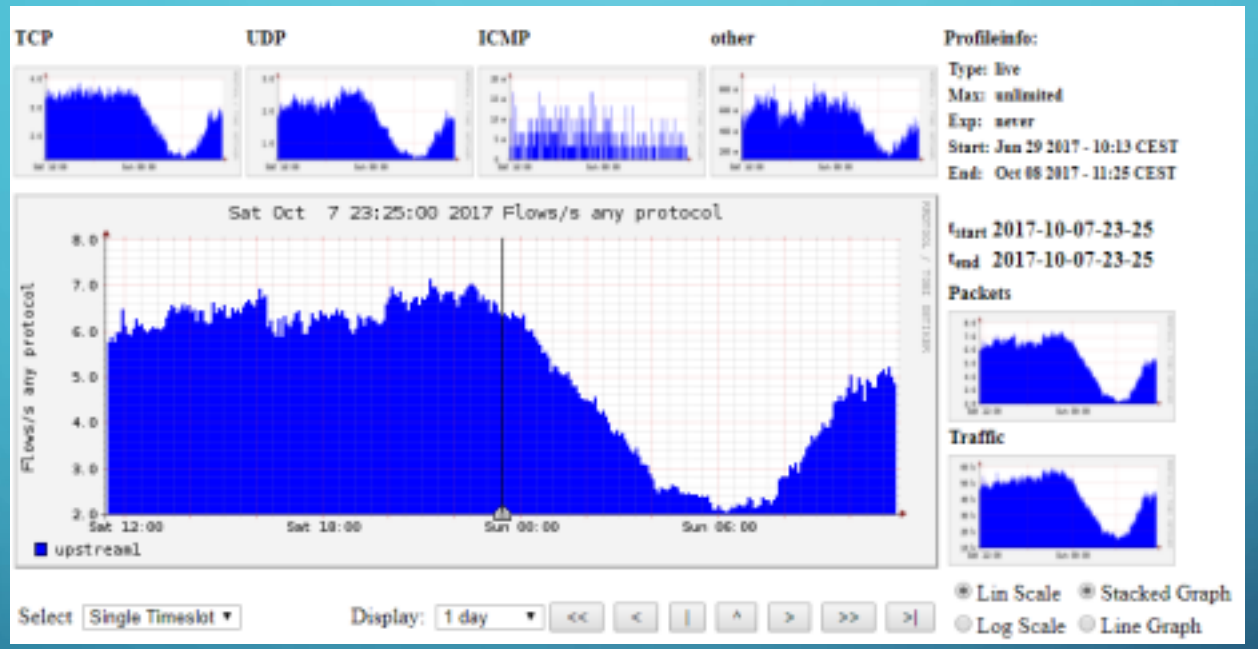
- 02.01 ERVERU



ADMINISTRACE ÚSTAVNÍCH SÍTÍ – CO SE V SÍTI DĚJE?

- NASAZENÍ MONITORINGU AKTIVNÍCH SÍTOVÝCH PRVKŮ
- NASAZENÍ ANALÝZY SÍŤOVÝCH DAT
  - FlowMon
  - GreyCortex
  - NfSen – Netflow Sensor

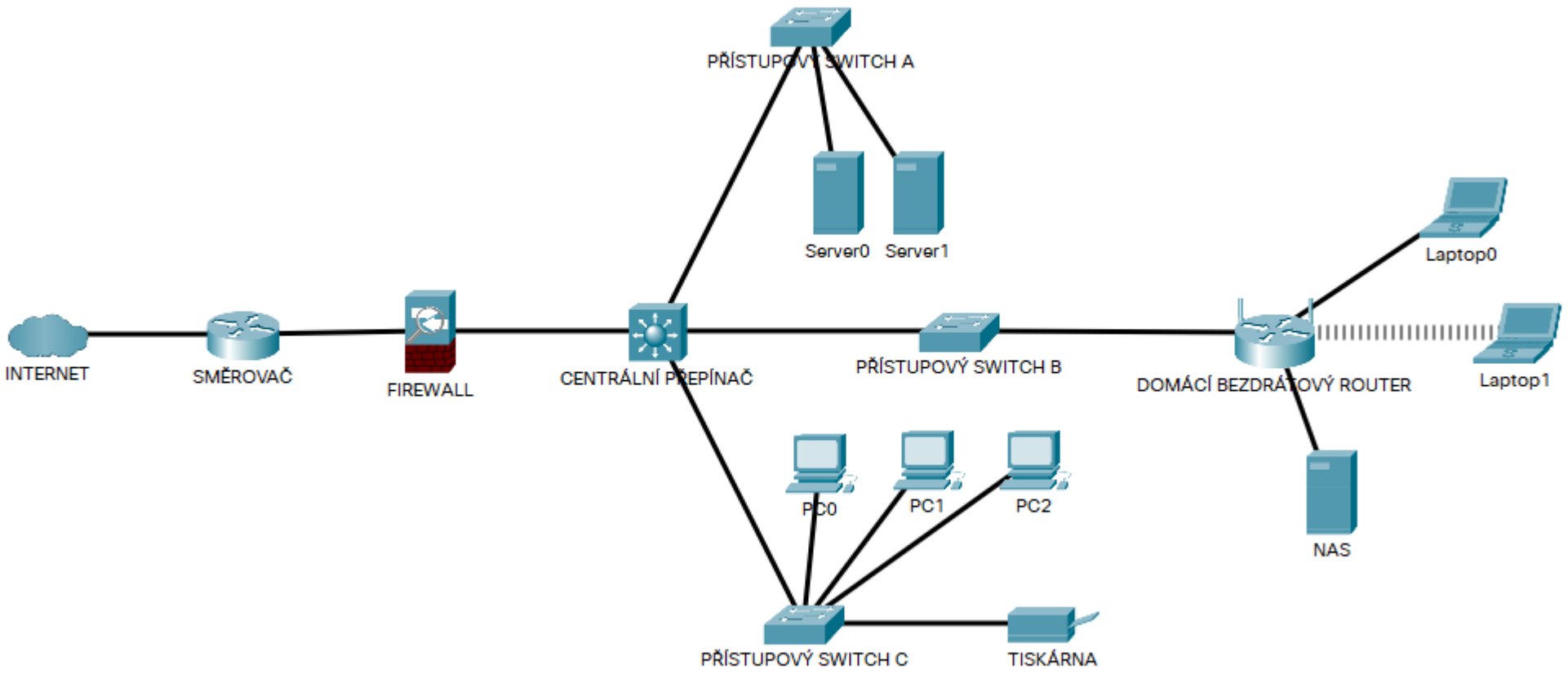
ADMINISTRACE ÚSTAVNÍCH SÍTÍ – CO SE V SÍTI DĚJE?



ADMINISTRACE ÚSTAVNÍCH SÍTÍ – CO SE V SÍTI DĚJE?

	NetFlow-lite	Flexible NetFlow	sFlow
Technology	Flow-based	Flow-based	Packet-based
Sampling	Sampling (1 in 32, configurable)	Every packet accounted for	Sampling (1 in hundreds to thousands*)
Export format	V9 and IPFIX	V5, V9 and IPFIX	sFlow v5
Ecosystem	NetFlow Collector	NetFlow Collector	sFlow Collector
Availability	Cisco Catalyst 2960-X, 2960-XR, 2960-CX, and 3560-CX Series Switches, and Catalyst 4948E Ethernet Switch	Cisco Catalyst 3K, 4K, 6KCisco Nexus routers 7K, 2K, 1KV	Cisco Nexus 3K

ADMINISTRACE ÚSTAVNÍCH SÍTÍ



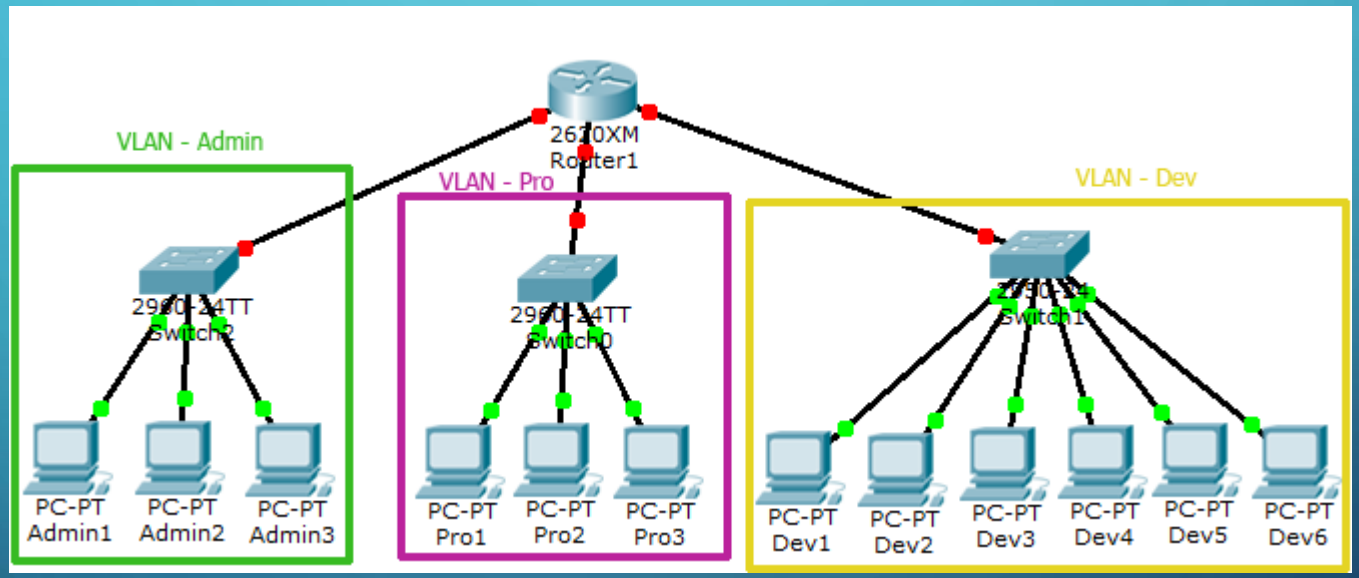
ADMINISTRACE ÚSTAVNÍCH SÍTÍ – CO SE V SÍTI DĚJE?

- NASAZENÍ MONITORINGU AKTIVNÍCH SÍTOVÝCH PRVKŮ
  - ZABBIX / ICINGA / Nagios
- NASAZENÍ ANALÝZY SÍŤOVÝCH DAT
  - NfSen – Netflow Sensor
    - Závěr: budeme muset segmentovat

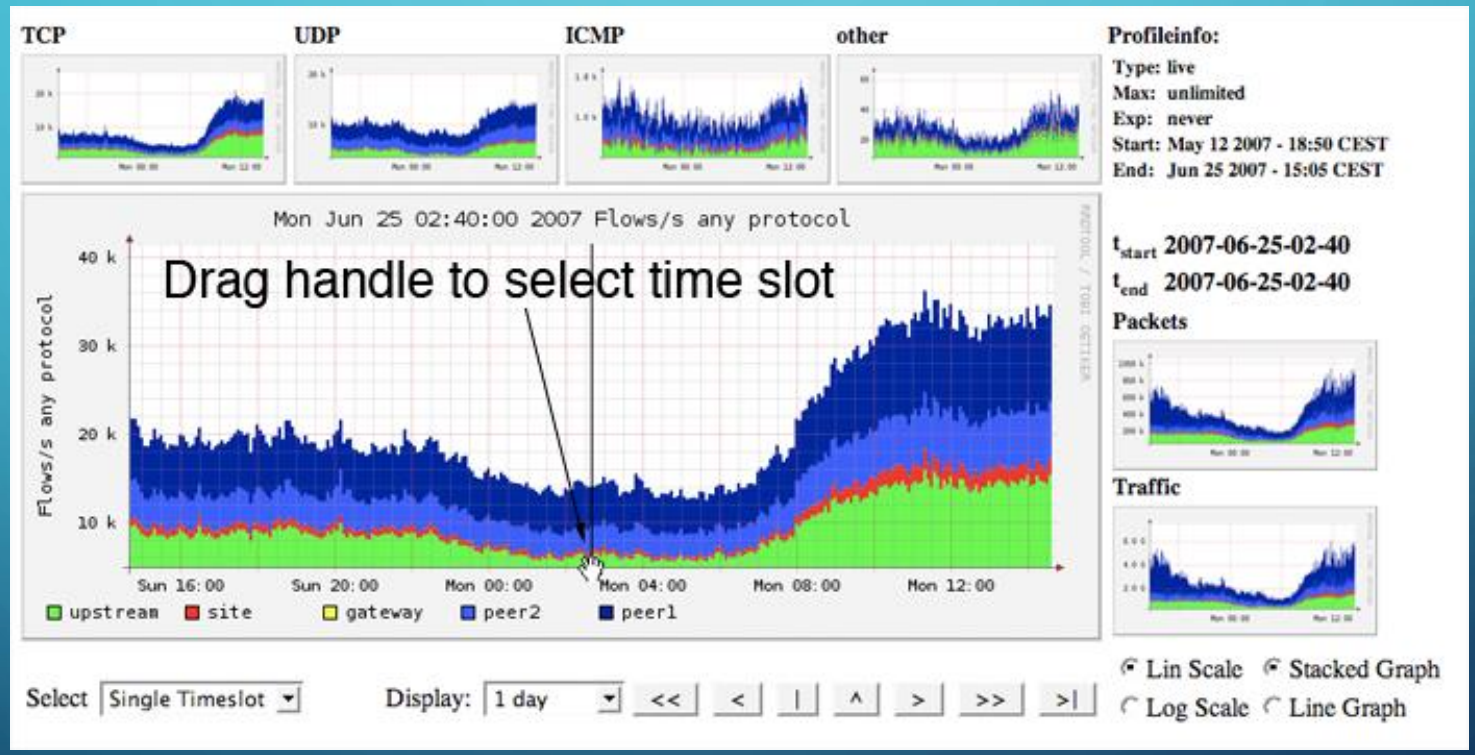
ADMINISTRACE ÚSTAVNÍCH SÍTÍ – CO SE V SÍTI DĚJE?

- NASAZENÍ MONITORINGU AKTIVNÍCH SÍTOVÝCH PRVKŮ
  - ZABBIX / ICINGA / Nagios
- NASAZENÍ ANALÝZY SÍŤOVÝCH DAT
  - NfSen – Netflow Sensor
    - Závěr: budeme muset segmentovat
      - Vhodný adresní plán

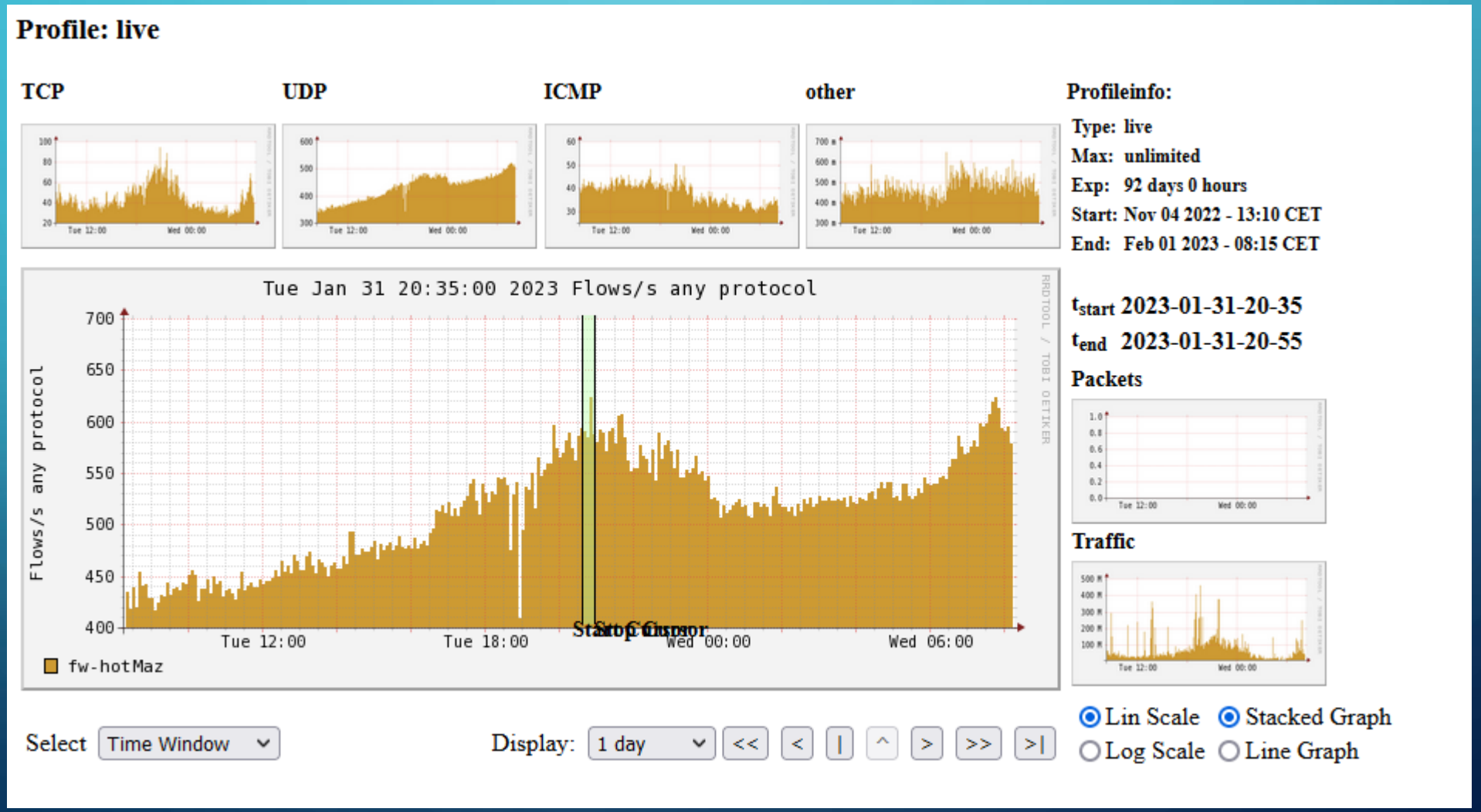
ADMINISTRACE ÚSTAVNÍCH SÍTÍ – BUDEME MUSET SEGMENTOVAT



ADMINISTRACE ÚSTAVNÍCH SÍTÍ



ADMINISTRACE ÚSTAVNÍCH SÍTÍ



ADMINISTRACE ÚSTAVNÍCH SÍTÍ

- 23.12.2034 – 17:35 – KOMUNIKACE S C&C BOTNETU
  - DST IP 18.214.21.235

```
nfdump filter:
dst ip 18.214.21.235
Date first seen          Event  XEvent Proto      Src IP Addr:Port          Dst IP Addr:Port     X-Src IP Addr:Port        X-Dst IP Addr:Port   In Byte Out Byte
2023-01-31 20:35:16.041 CREATE  Ignore TCP       10.2.24.145:41222 ->    18.214.21.235:443     147.231.17.106:41222 ->    18.214.21.235:443         0        0
2023-01-31 20:35:16.041 UPDATE  Ignore TCP       10.2.24.145:41222 ->    18.214.21.235:443     147.231.17.106:41222 ->    18.214.21.235:443      1821    15809
2023-01-31 20:36:17.853 UPDATE    2031 TCP       10.2.24.145:41222 ->    18.214.21.235:443     147.231.17.106:41222 ->    18.214.21.235:443         0       24
2023-01-31 20:35:16.041 DELETE    2031 TCP       10.2.24.145:41222 ->    18.214.21.235:443     147.231.17.106:41222 ->    18.214.21.235:443      1821    15833
Summary: total flows: 4, total bytes: 35308, total packets: 0, avg bps: 4569, avg pps: 0, avg bpp: 0
Time window: 2023-01-25 17:19:44 - 2023-01-31 21:00:00
Total flows processed: 3989485, Blocks skipped: 0, Bytes read: 463802692
Sys: 0.980s flows/second: 4067375.2  Wall: 0.961s flows/second: 4149100.9
```

ADMINISTRACE ÚSTAVNÍCH SÍTÍ

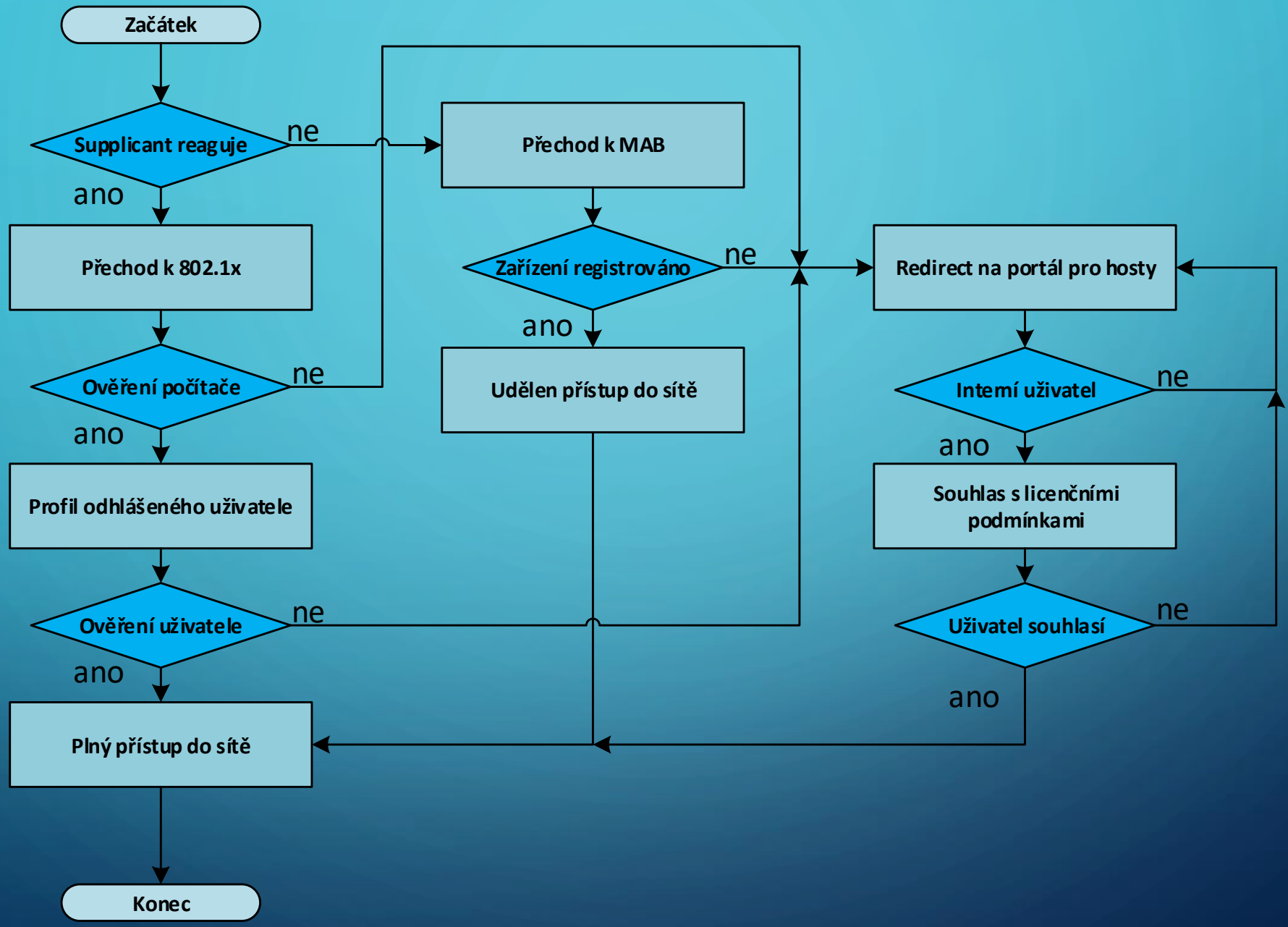
- 23.12.2034 – 17:35 – KOMUNIKACE S C&C BOTNETU
  - DST IP 18.214.21.235
    - Kdo to vlastně je?
      - Implementace řízení přístupu do sítě - od toho se dále odvijí
      - Logování NAT
      - Logování DHCP zpráv

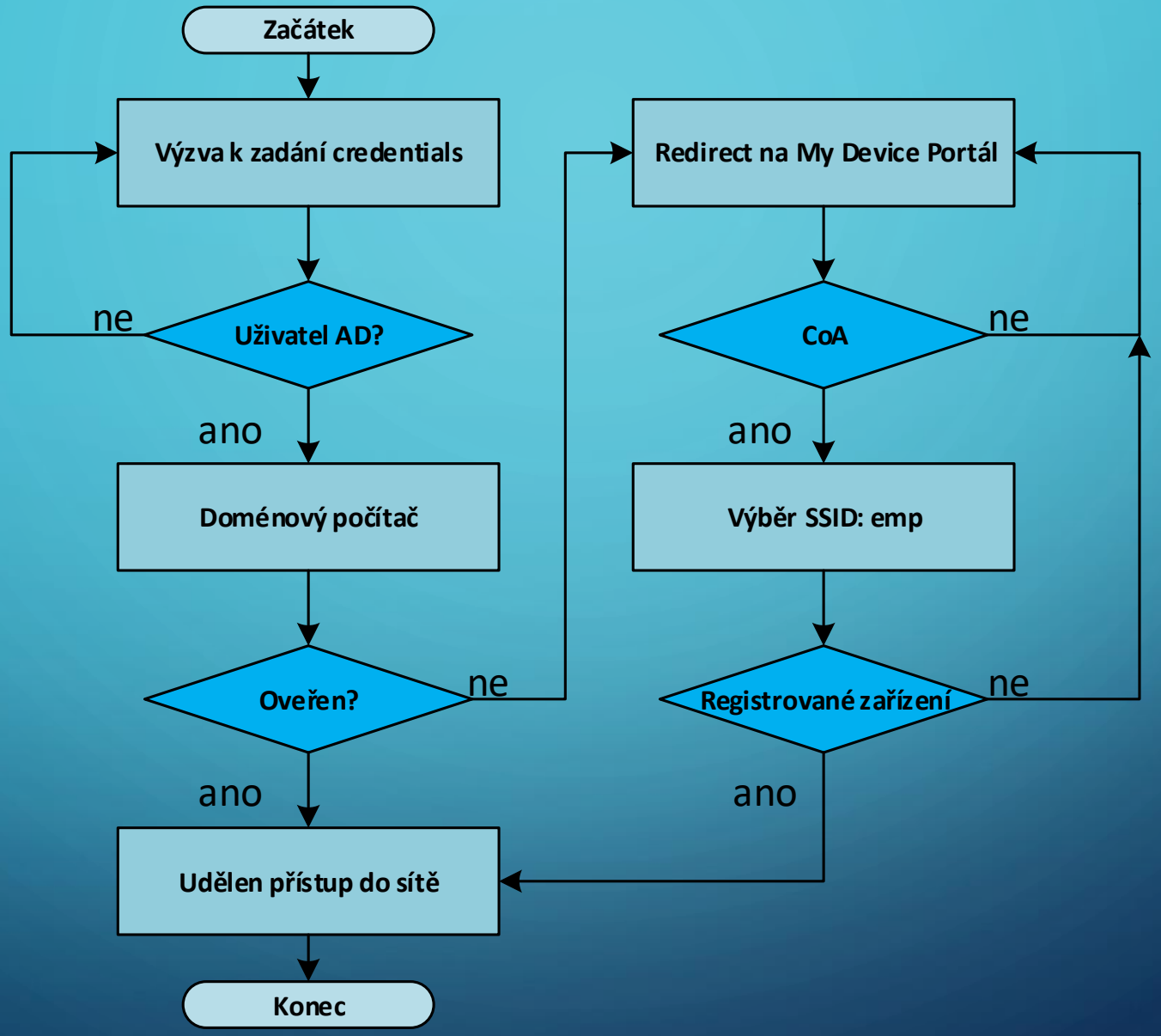
BEZPEČNOST ÚSTAVNÍHO IT

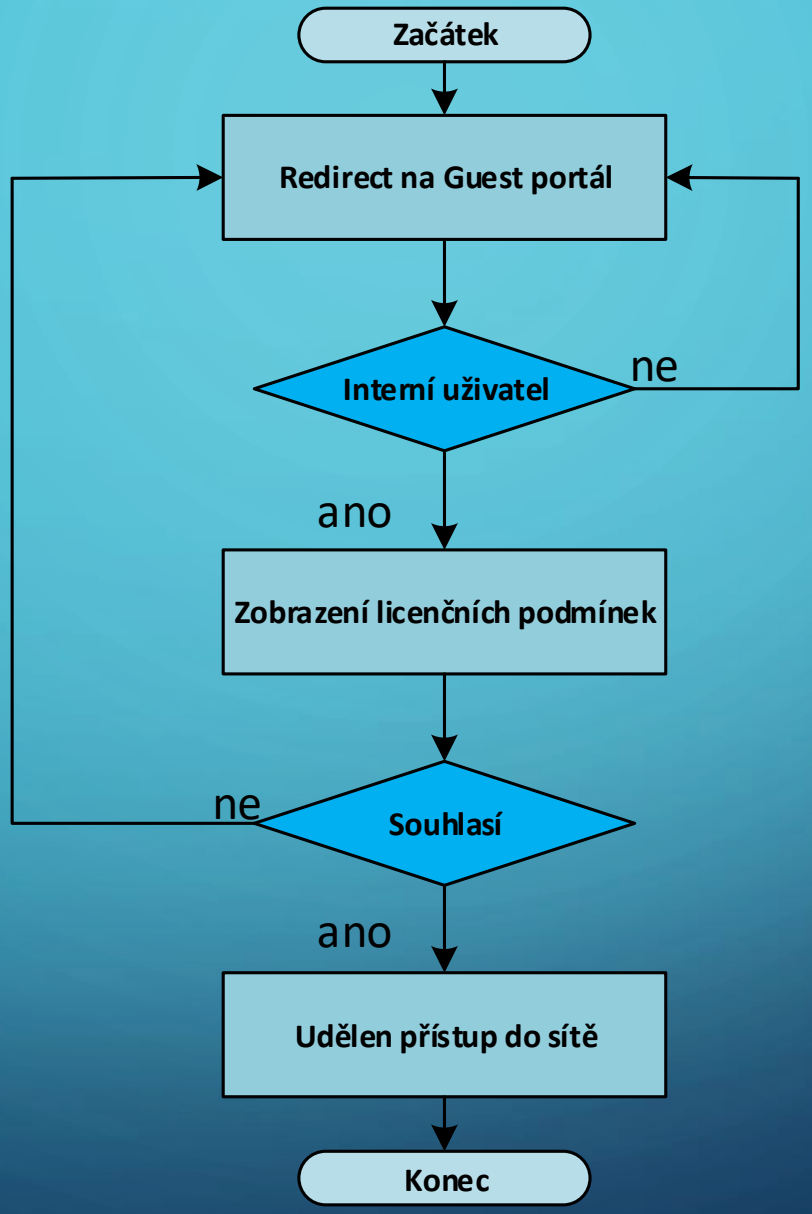
- Systému redundance firewallu - z důvodu velkých pořizovacích nákladu provozujeme jen jeden
  - Více jak 12 lokalit od 10 do 200 uživatelů
  - HA řešení: Datacentra, Národní
  - Ostatní lokality: Dá nám na to vedení peníze? / Považují výpadek do následujícího pracovního dne krytický?
    - Držíme na skladě starší, nicméně stále funkční zařízení

BEZPEČNOST ÚSTAVNÍHO IT

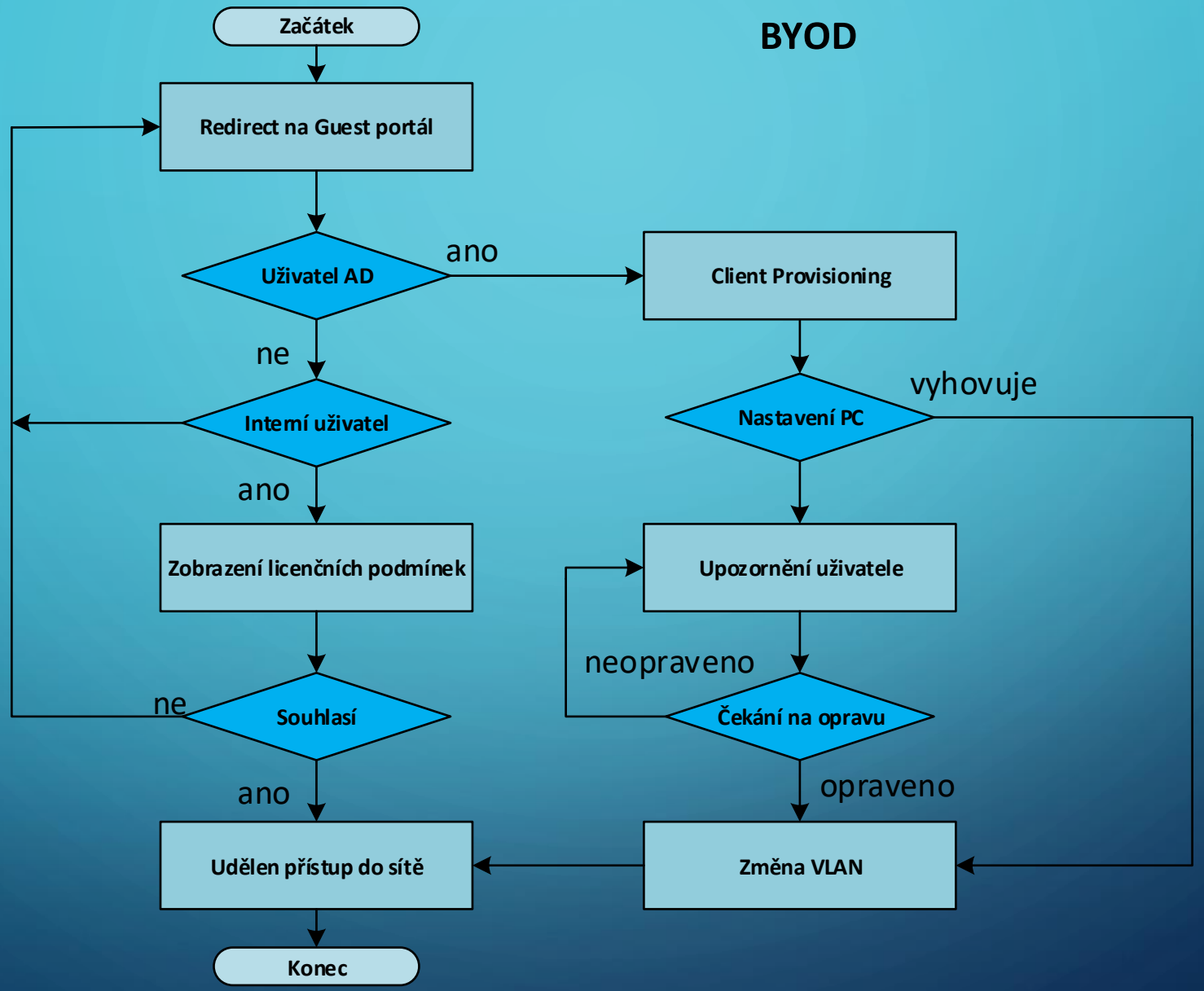
- Implementace řízení přístupu do sítě - od toho se dále odvijí


Začátek
Supplicant reaguje
ne
ano
Přechod k MAB
Přechod k 802.1x
Zařízení registrováno
ne
ano
Redirect na portál pro hosty
Ověření počítače
ne
ano
Udělen přístup do sítě
Interní uživatel
ne
ano
Profil odhlášeného uživatele
Souhlas s licenčními podmínkami
Ověření uživatele
ne
ano
Uživatel souhlasí
ne
ano
Plný přístup do sítě
Konec


Začátek
Výzva k zadání credentials
Uživatel AD?
ne
ano
Doménový počítač
Ověřen?
ne
ano
Udělen přístup do sítě
Konec
Redirect na My Device Portál
CoA
ne
ano
Výběr SSID: emp
Registrované zařízení
ne
ano


Začátek
Redirect na Guest portál
Interní uživatel
ne
ano
Zobrazení licenčních podmínek
Souhlasí
ne
ano
Udělen přístup do sítě
Konec

BYOD


Začátek
Redirect na Guest portál
Uživatel AD
ano
Client Provisioning
ne
Interní uživatel
vyhovuje
Nastavení PC
ano
Zobrazení licenčních podmínek
Upozornění uživatele
neopraveno
ne
Souhlasí
Čekání na opravu
ano
opraveno
Udělen přístup do sítě
Změna VLAN
Konec

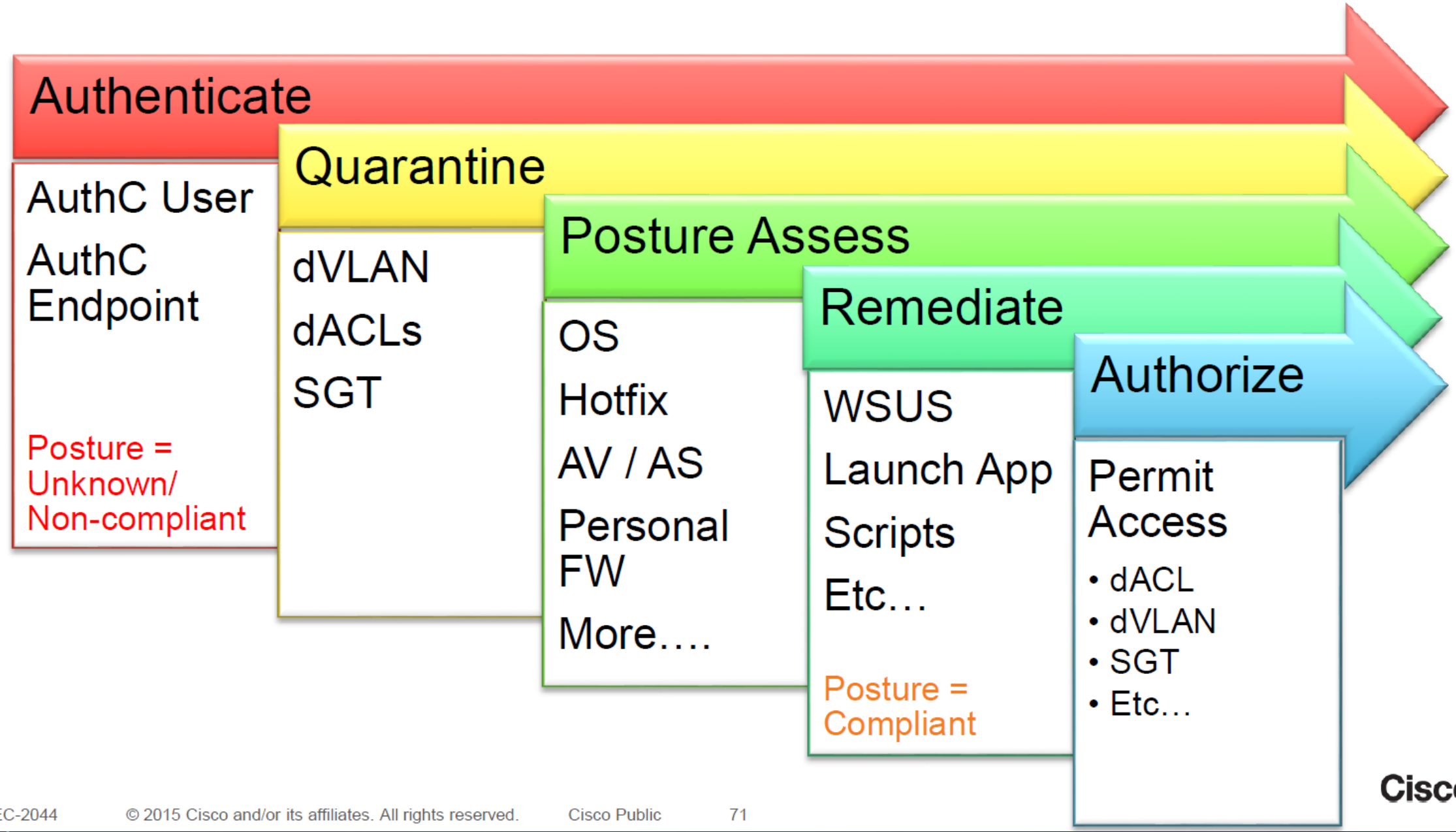
holec@ignacius:~

```
fa-utia-iselab#show mac address-table address 68f7.28af.98ed
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
  20    68f7.28af.98ed    STATIC      Gi0/8
Total Mac Addresses for this criterion: 1
fa-utia-iselab#show authentication sessions interface gigabitEthernet 0/8 details
            Interface:  GigabitEthernet0/8
          MAC Address:  68f7.28af.98ed
         IPv6 Address:  Unknown
         IPv4 Address:  10.7.20.150
            User-Name:  holec
               Status:  Authorized
               Domain:  DATA
       Oper host mode:  multi-auth
     Oper control dir:  both
      Session timeout:  N/A
      Restart timeout:  N/A
Periodic Acct timeout:  N/A
    Common Session ID:  0A07040B00000183B1C2F7A1
      Acct Session ID:  0x00000B43
               Handle:  0xF3000055
       Current Policy:  POLICY_Gi0/8

Local Policies:
        Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)

Server Policies:
           Vlan Group:  Vlan: 20
              ACS ACL:  xACSACLx-IP-PERMIT_ALL_IPV4_TRAFFIC-57f6b0d3

Method status list:
       Method           State

       dot1x            Authc Success

fa-utia-iselab#
```

BEZPEČNOST ÚSTAVNÍHO IT

- Systému redundance firewallu - z důvodu velkých pořizovacích nákladu provozujeme jen jeden
- Implementace řízení přístupu do sítě - od toho se dále odvijí
  - Jaké zařízení nám uživatelé připojují do sítě
  - Zabezpečeni jednotlivých PC (certifikat, token?) nyní na heslo, mnohdy trivialní, někdy ani to ne
  - Problémem je dozor nad tím, zda uživatelé linuxu řádně aktualizují.
  - Bezpečnost neaktualizovaných zařízení s Androidem.

ISE Posture Assessment



BEZPEČNOST ÚSTAVNÍHO IT

- Systému redundance firewallu - z důvodu velkých pořizovacích nákladu provozujeme jen jeden
- Implementace řízení přístupu do sítě - od toho se dále odvijí
- Zabezpečeni jednotlivých PC (certifikat, token?) nyní na heslo, mnohdy trivialní, někdy ani to ne
  - Zavedení LDAP / AD -> 2FA certifikát
- Problémem je dozor nad tím, zda uživatelé linuxu řádně aktualizují.
  - Inventarizační SW -> ITAM - **IT Asset Management Software**
- Bezpečnost neaktualizovaných zařízení s Androidem.
  - Bez MDM prakticky nemožné – budeme pokračovat kapitolou ústavní legislativy

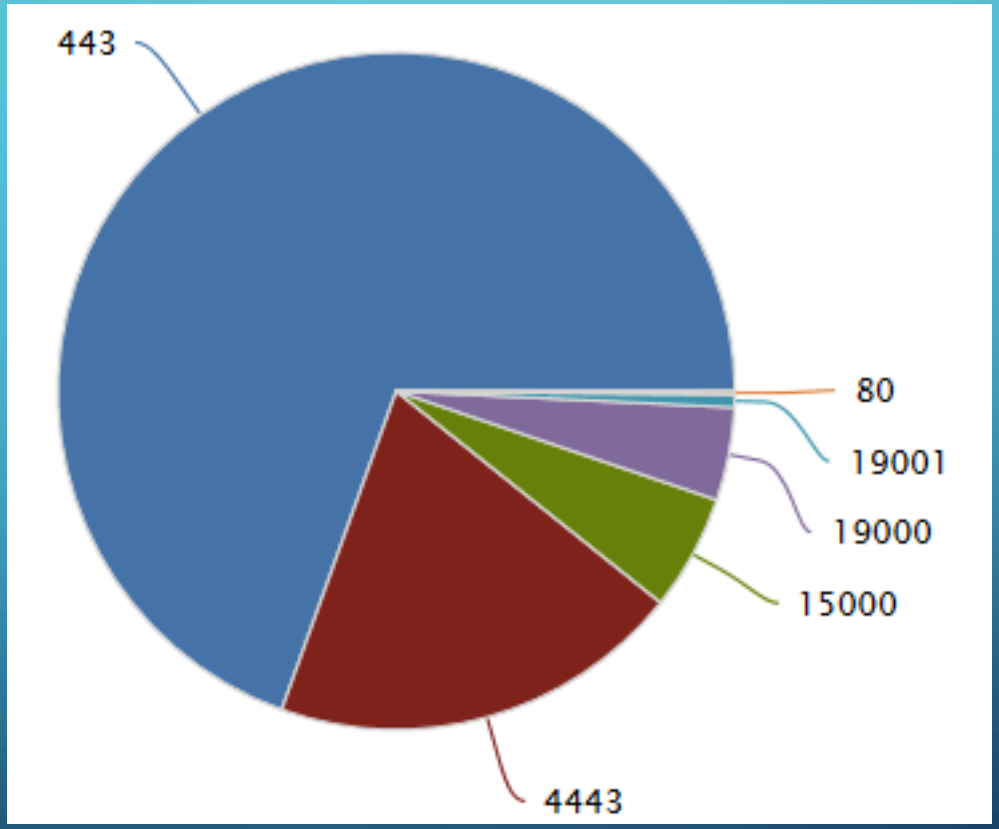
BEZPEČNOST ÚSTAVNÍHO IT

BEZPEČNOST ÚSTAVNÍHO IT

- Používání vlastních zařízení (BYOD)
  - Jak zařízení spravovat
    - Bude nutné nasazení technologie MDM
- AirWatch -> **VMWare Workspace ONE**
- **Ivanti MobileIron**
- **Citrix Endpoint Management**
- **Headwind MDM – OpenSource**

BEZPEČNOST ÚSTAVNÍHO IT

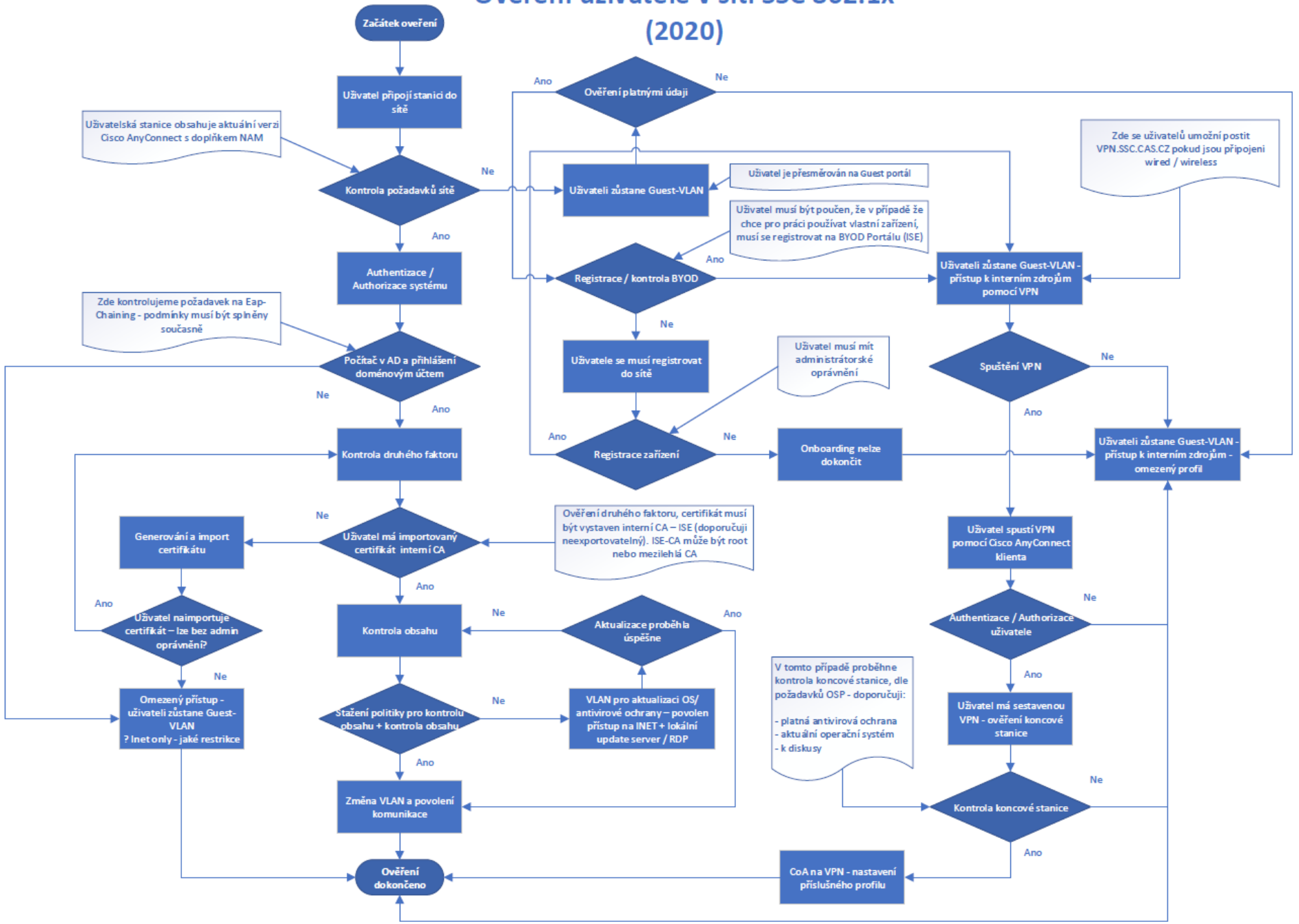
- SSL dekrypce



MOHLO BY TO TAKTO VYPADAT?

- Segmentace sítě – plochá síť = špatná síť
  - zavedení migrosegmentace – privátní VLAN / Always-On VPN
- Síťové sondy – ne vždy se musí jednat o velkou investici
- Základní bezpečnostní mechanizmi sítě
  - IP DHCP snooping
  - IP ARP inspection
  - Port security
- Logujte kdo co dělá
  - Analýza logů – dedikovaný lidský zdroj / siem
- Redundance
- Zavedení ověřování uživatelů 802.1x
- Zavedení SSL dekrypce

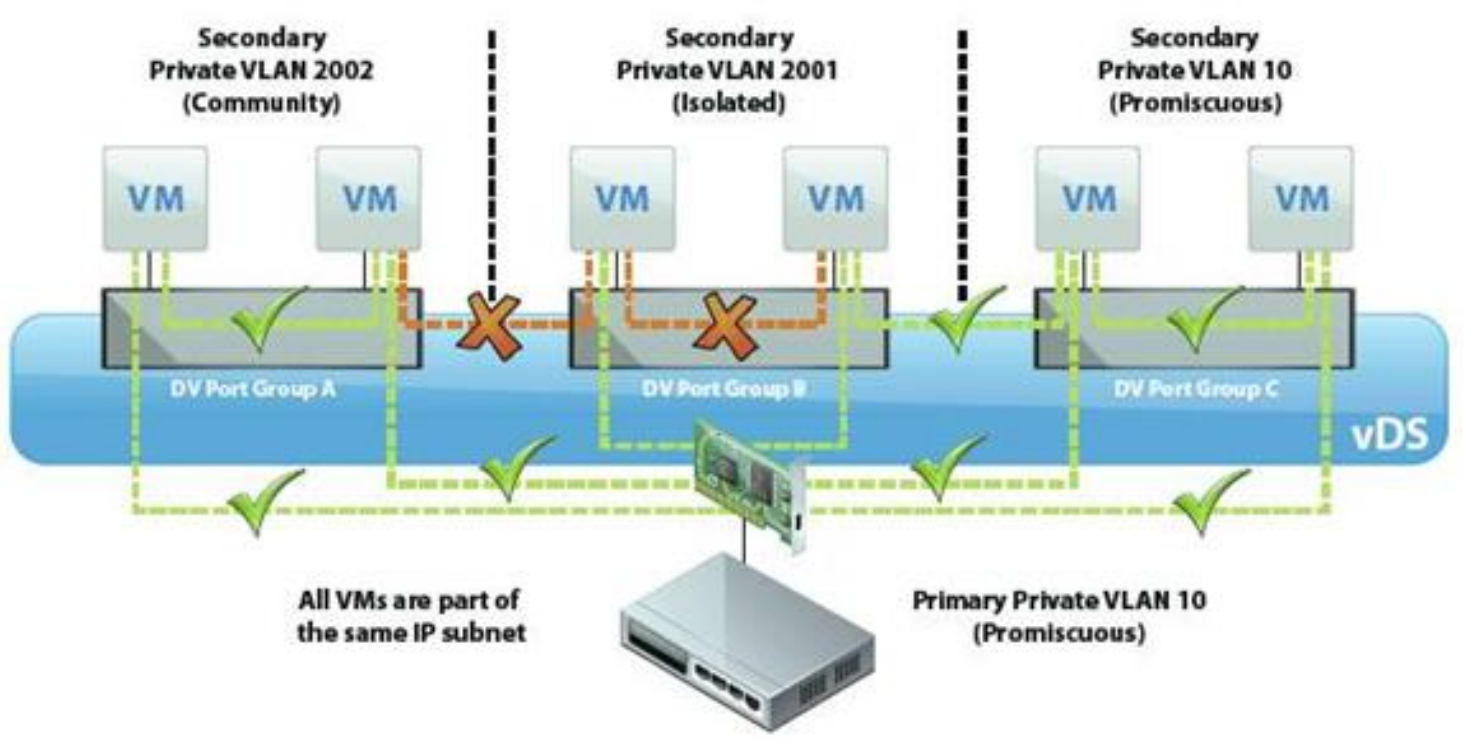
Ověření uživatele v síti SSČ 802.1x (2020)

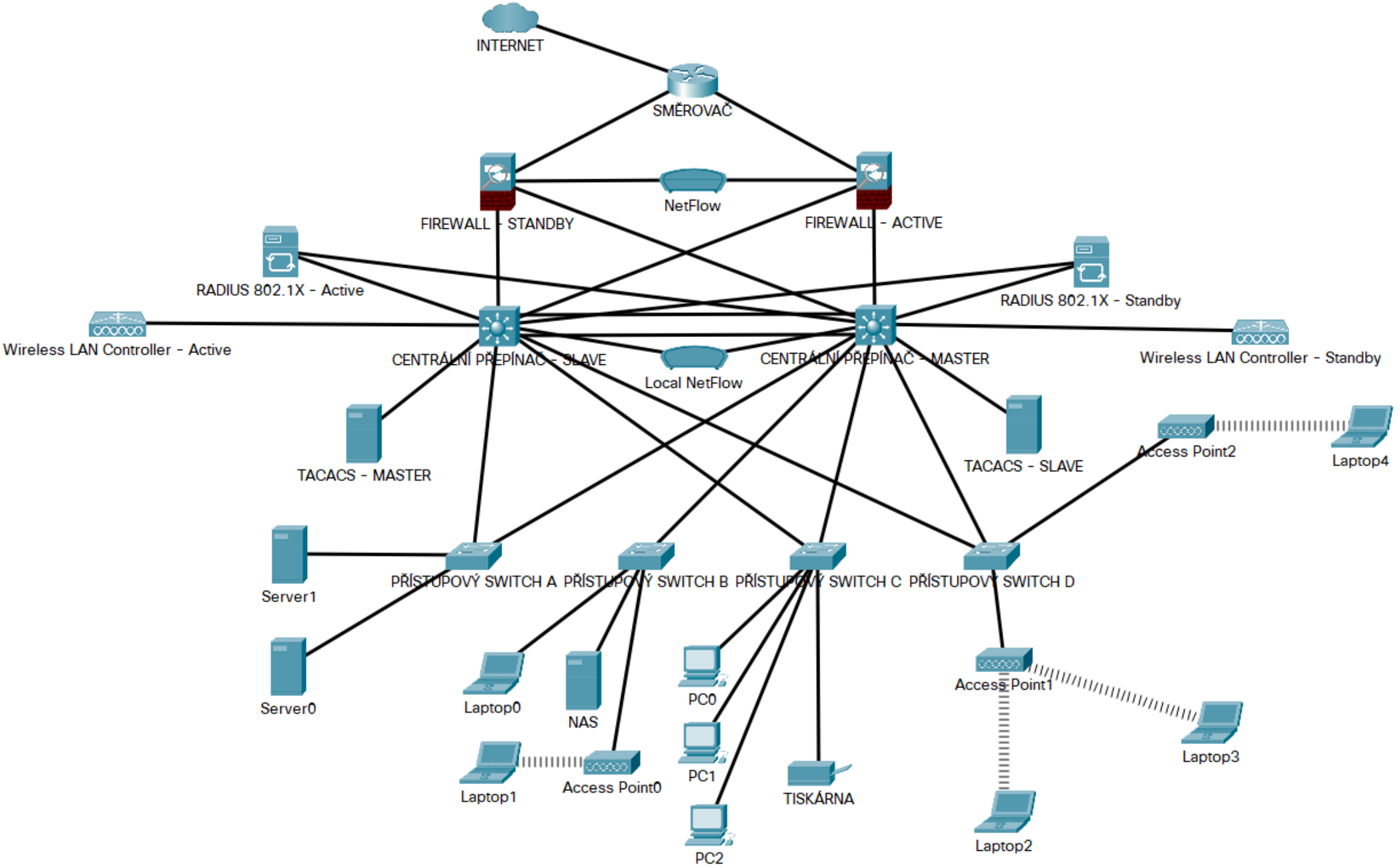


ÚSTAVNÍ LEGISLATIVA

- Používání vlastních zařízení (BYOD)
  - Centrální nákup zařízení / věcné schválení
  - Směrnice pro provoz zařízení na ústavní síti

ZAVEDENÍ MIGROSEGMENTACE – PRIVÁTNÍ VLAN




INTERNET
SMĚROVAČ
FIREWALL - STANDBY
NetFlow
FIREWALL - ACTIVE
RADIUS 802.1X - Active
RADIUS 802.1X - Standby
Wireless LAN Controller - Active
CENTRÁLNÍ PŘEPÍNAČ - SLAVE
Local NetFlow
CENTRÁLNÍ PŘEPÍNAČ - MASTER
Wireless LAN Controller - Standby
TACACS - MASTER
TACACS - SLAVE
Access Point2
Laptop4
Server1
PŘÍSTUPOVÝ SWITCH A
PŘÍSTUPOVÝ SWITCH B
PŘÍSTUPOVÝ SWITCH C
PŘÍSTUPOVÝ SWITCH D
Server0
Laptop0
NAS
PC0
Access Point1
Laptop3
PC1
Laptop1
Access Point0
TISKÁRNA
Laptop2
PC2

DĚKUJI ZA POZORNOST