Network discovery
s využitím protokolu SNMP

Tomáš Řehořek

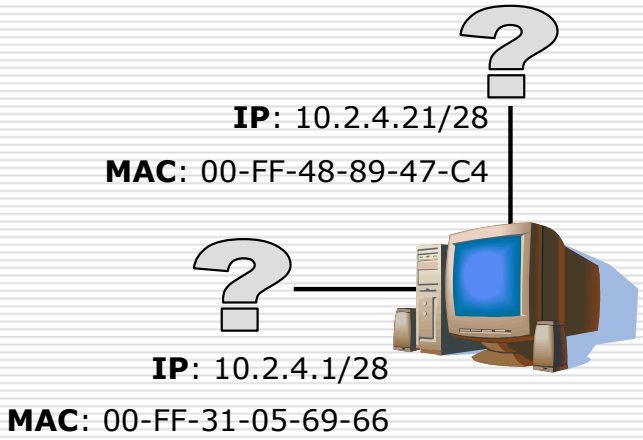
Možná řešení

- broadcast ping
  - často se vyhodnocuje jako **útok**
  - mnoho systémů (MS Windows) na něj při výchozím nastavení neodpovídá
  - nevhodné řešení
- DNS zone transfer
  - AXFR query (stažení seznamu celé domény)
  - potenciální bezpečnostní riziko, DNS server by neměl mít veřejně povoleno
  - nevhodné řešení z mnoha důvodů
- …SNMP?

SNMP

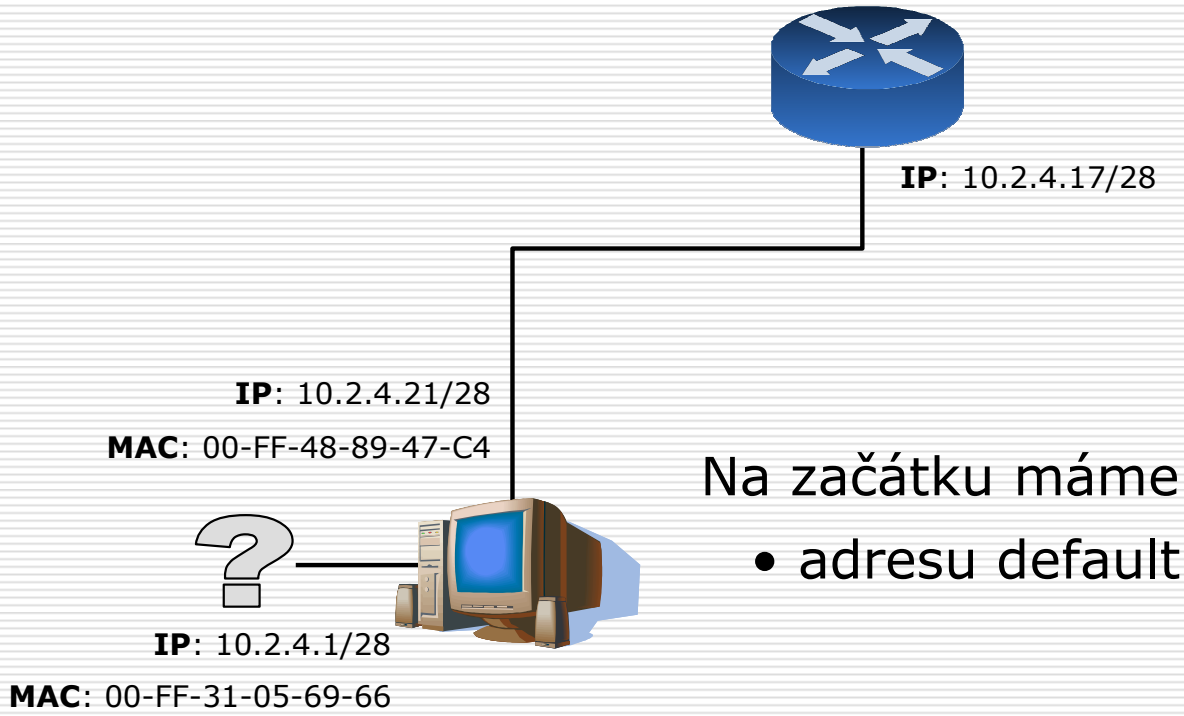
- Address Translation Table
  - definována v RFC 1213 (MIB-II)
  - de facto abstrakce nad ARP cache
  - jejím stažením obdržíme dvojice: (fyzická adresa, IP adresa)
- toto řešení si zde rozebereme

Výchozí bod algoritmu



Na začátku máme:

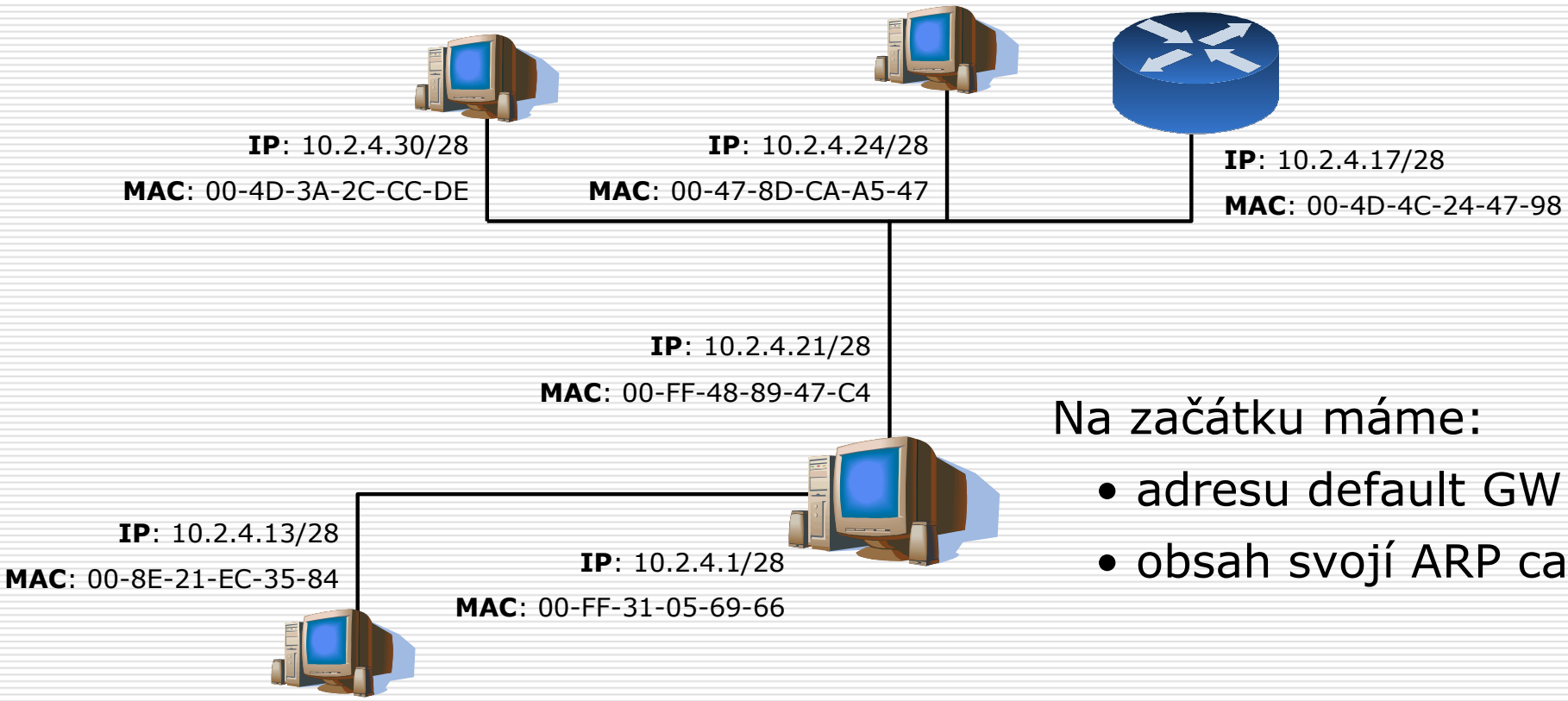
Výchozí bod algoritmu



Na začátku máme:

- adresu default GW

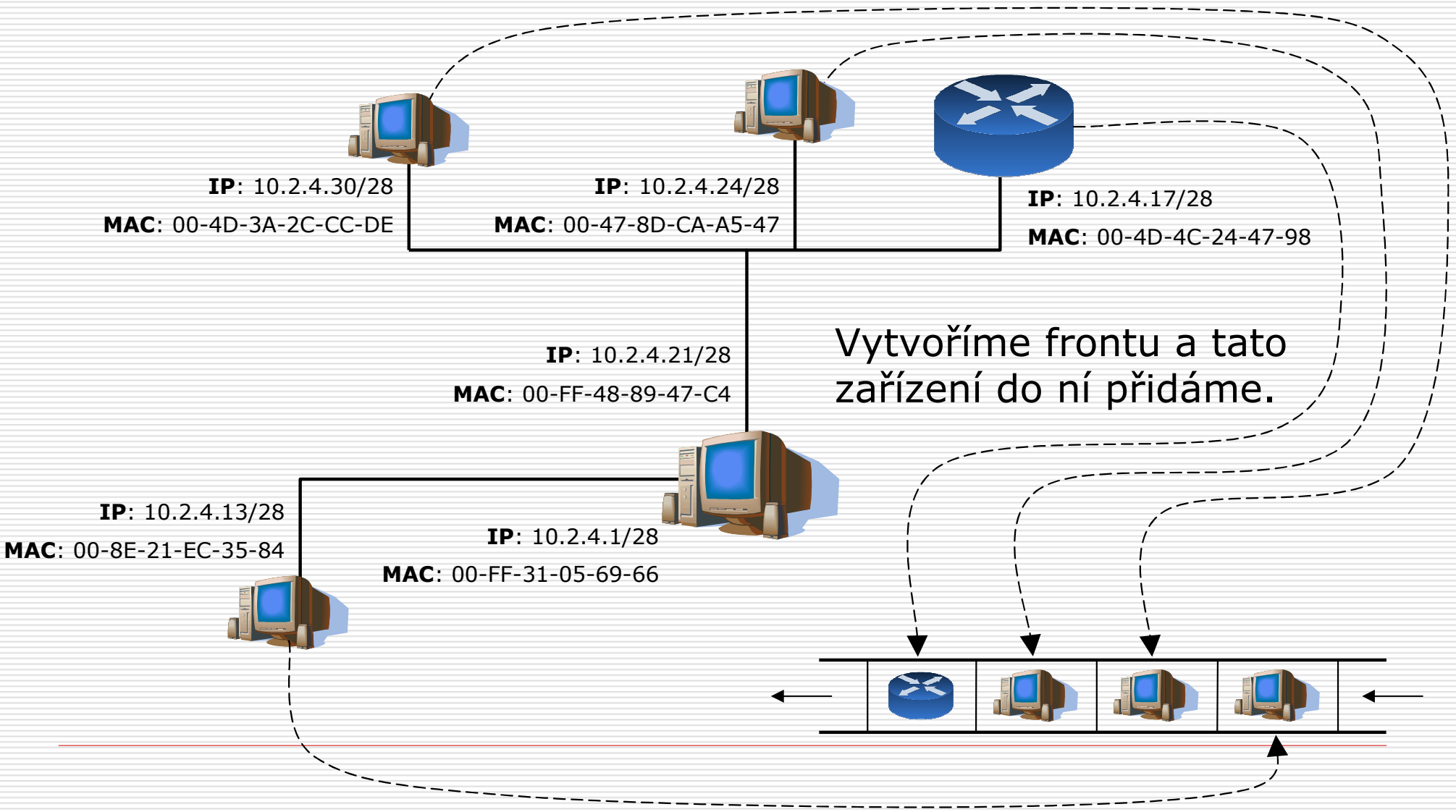
Výchozí bod algoritmu



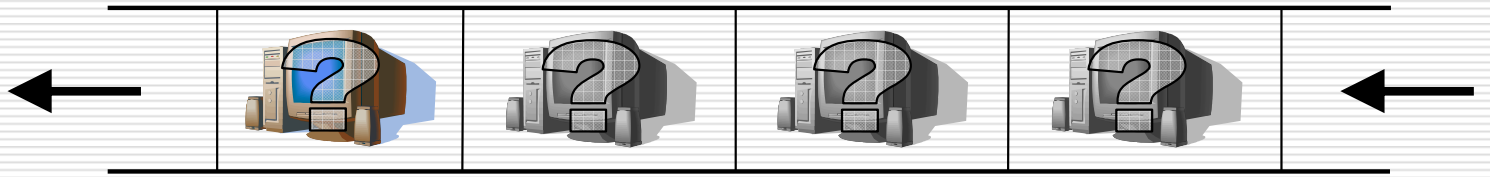
Na začátku máme:

- adresu default GW
- obsah svojí ARP cache

Výchozí bod algoritmu



Běh algoritmu



- Dokud jsou ve frontě nějaká zařízení, odebíráme vždy první a to zpracujeme

Zpracování zařízení

- zkusíme přes SNMP získat `sysObjectID`
- v případě úspěchu víme, že na zařízení běží SNMP a zároveň získáme typ zařízení; v závislosti na typu zařízení poté můžeme vyžádat další informace
- v případě neúspěch můžeme zkusit alespoň unicast ping, abychom zjistili, zda je zařízení v provozu

Vyžádání dalších informací

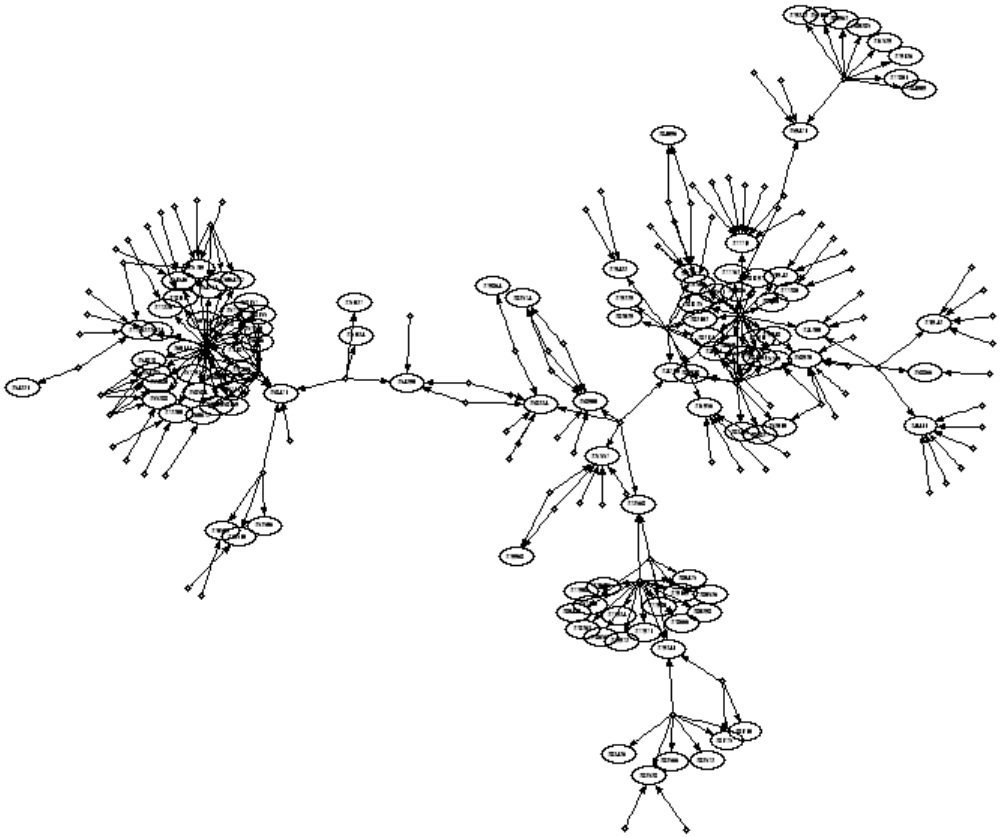
- od zařízení operujícího na **3. vrstvě** vyžádáme:
  - seznam místních portů, jejich HW adres a přidělených IP adres (vztah typu 1:N)
  - obsah ARP cache; takto nalezená zařízení opět přidáme do fronty ke zpracování
- od zařízení operujícího na **2. vrstvě** vyžádáme:
  - seznam portů pro správu, jejich HW adres a k nim příslušných IP adres
  - seznam portů a k nim příslušných HW adres (RFC 1493 – Definitions of managed objects for bridges: `dot1dTpFdbTable`)

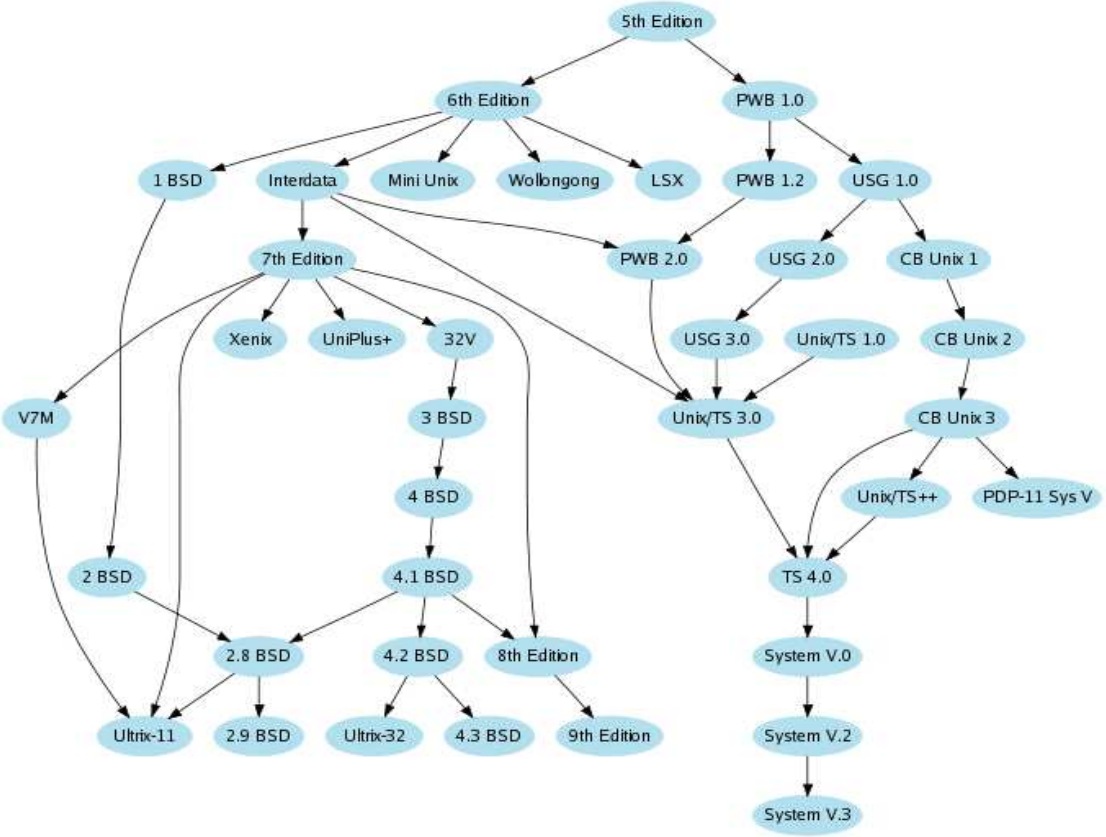
Související problémy

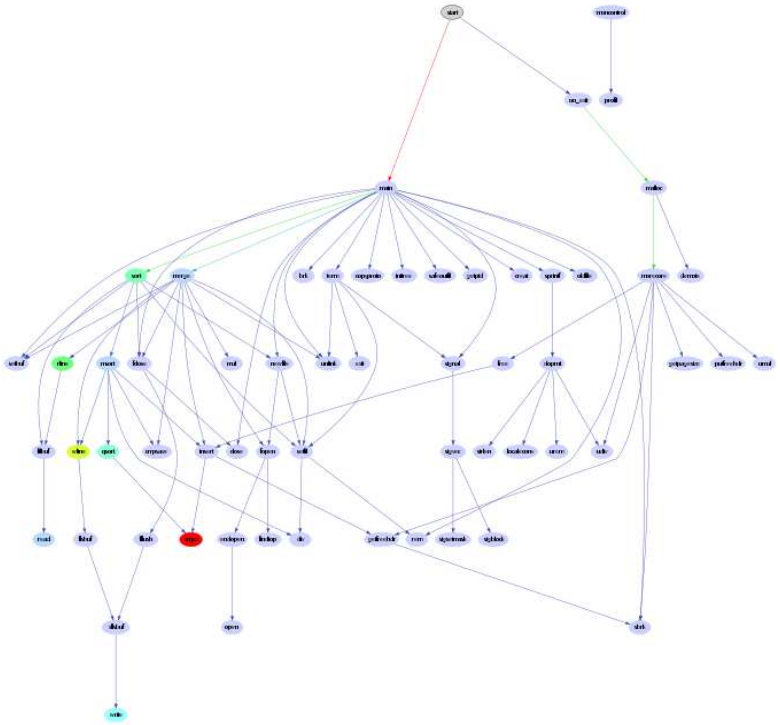
- nesmíme prohledávat celý internet
  - v případě, že najdeme nový segment, musíme od uživatele vyžádat souhlas k jeho zkoumání
  - je vhodné udržovat seznam segmentů, jejichž zkoumání již uživatel zakázal
- má-li zařízení více IP adres
  - …a zároveň s námi nekomunikuje přes SNMP, pouze odpoví na ping, nevyhodnotíme to jako jediné zařízení

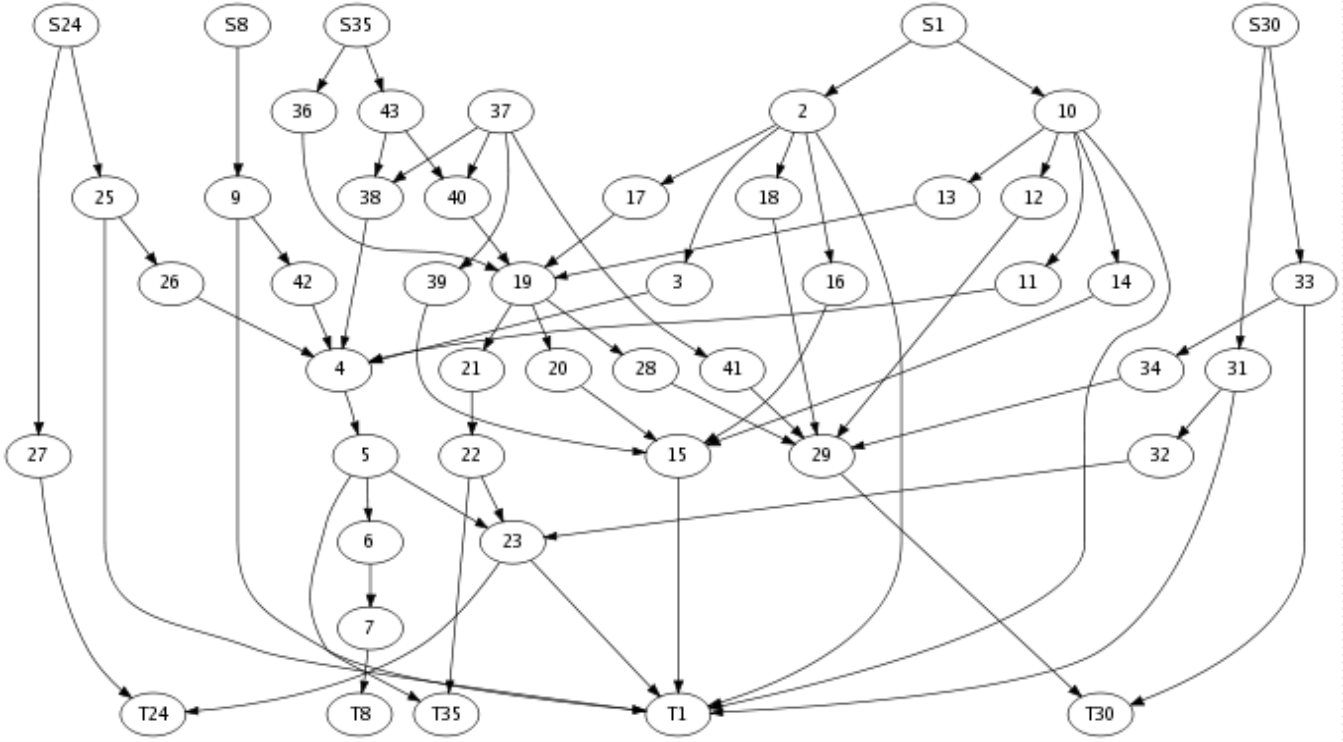
Jak na vykreslení grafu?

- např. http://www.graphviz.org/
- již zastavený přidružený projekt **Grappa** – sada knihoven pro Javu
- ukázka na další průsvitce




5th Edition
6th Edition
PWB 1.0
1 BSD
Interdata
Mini Unix
Wollongong
LSX
PWB 1.2
USG 1.0
7th Edition
PWB 2.0
USG 2.0
CB Unix 1
Xenix
UniPlus+
32V
USG 3.0
Unix/TS 1.0
CB Unix 2
V7M
3 BSD
Unix/TS 3.0
CB Unix 3
4 BSD
Unix/TS++
PDP-11 Sys V
2 BSD
4.1 BSD
TS 4.0
2.8 BSD
4.2 BSD
8th Edition
System V.0
Ultrix-11
2.9 BSD
Ultrix-32
4.3 BSD
9th Edition
System V.2
System V.3




S24
S8
S35
S1
S30
36
43
37
2
10
25
9
38
40
17
18
13
12
26
42
39
19
3
16
11
14
33
4
21
20
28
41
34
31
27
5
22
15
29
32
6
23
7
T24
T8
T35
T1
T30

Děkuji za pozornost.