



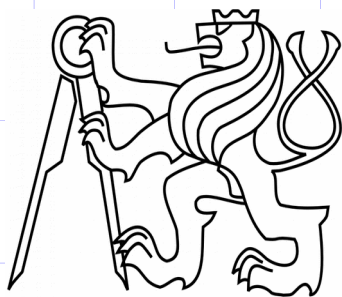
# Správa sítí

RNDr. Ing. Vladimír Smotlacha, Ph.D.

Katedra počítačových systémů  
Fakulta informačních technologií  
České vysoké učení technické v Praze  
© Vladimír Smotlacha, 2017

Počítačové sítě BI-PSI  
LS 2017/18, Předn. 12

<https://edux.fit.cvut.cz/BI-PSI>

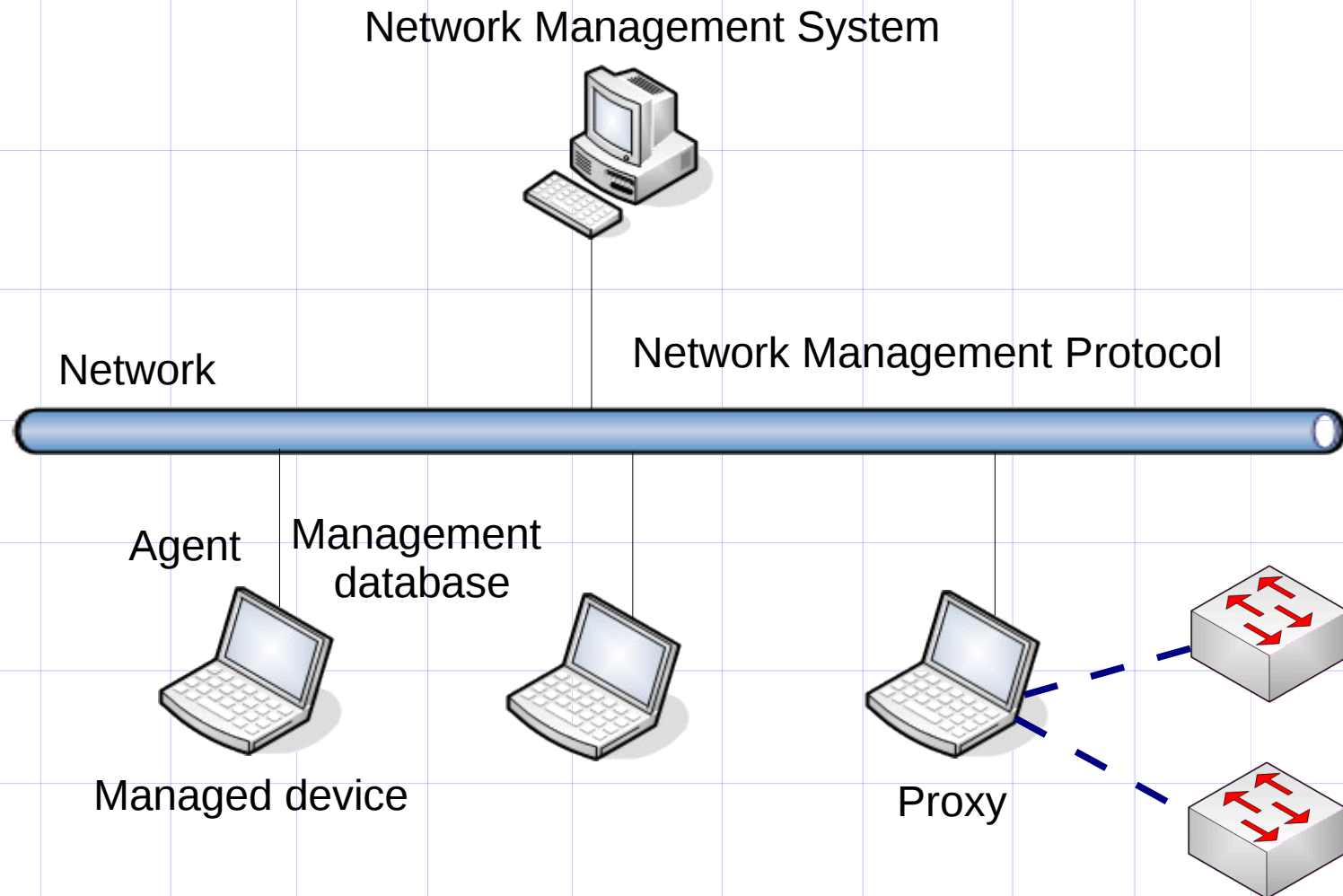




# Síťová správa podle ISO

- správa výkonu (performance management)
  - reaktivní a proaktivní
  - měření výkonnosti a zatížení
- správa konfigurace (configuration management)
  - monitorování síťové konfigurace
- účetní správa (accounting management)
  - monitorování využití sítě
- správa poruch a chyb (fault management)
  - detekce chyb, logování a oznámení
- správa bezpečnosti (security management)
  - nastavení a monitorování přístupu

# Architektura





# Monitorování

- stav linek a síťových prvků
  - funkčnost, zatížení, ...
- routování
  - mapy, jejich změny, ...
- identifikace protokolů
  - číslo portu
  - charakteristika toků (objem dat, časování, ...)
  - samoučící metody
- sledování parametrů (QoS)
  - zpoždění, jitter, volné pásmo, ...



# NetFlow

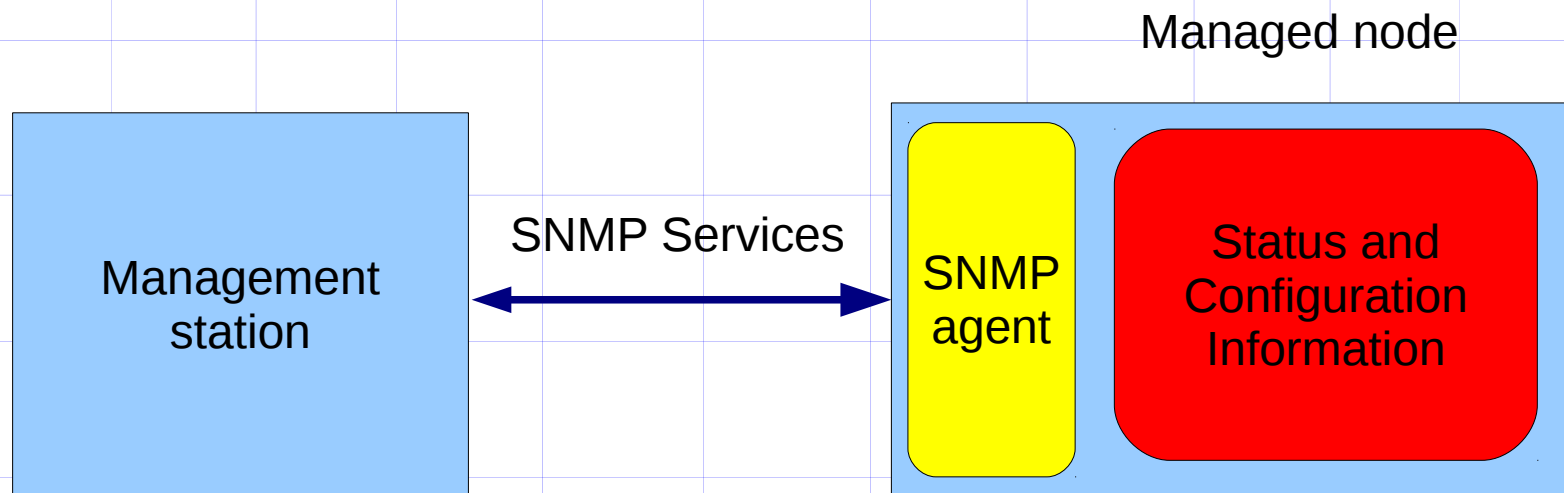
- sledování informací o datových tocích (flow-based)
  - flow: shoduje se zdrojová/cílová adresa, port, protokol, ToS
- vývoj a implementace Cisco, později standard IETF
- podpora na síťových prvcích
  - export dat o datových tocích
- možnost vzorkování
  - deterministicky: každý  $n$ -tý paket
  - náhodně: jeden paket z  $n$



# SNMP

- Simple Network Management Protocol
  - UDP / 161
- orientováno na síťová zařízení (device-based)
- vývoj:
  - SNMPv1 – RFC1157
  - SNMPv2 – RFC1441
    - rozšířená bezpečnost
    - další operace
  - SNMPv2c – RFC1901
  - SNMPv3 – RFC3411

# SNMP model





# SNMP protokol

## Základní příkazy

- GetRequest
  - žádost o zaslání stavu/hodnoty objektu
- SetRequest
  - příkaz k nastavení hodnoty
- GetNextRequest
  - žádost o informaci o následujícím objektu
- Response
  - odpověď
- Trap
  - asynchronní upozornění na událost



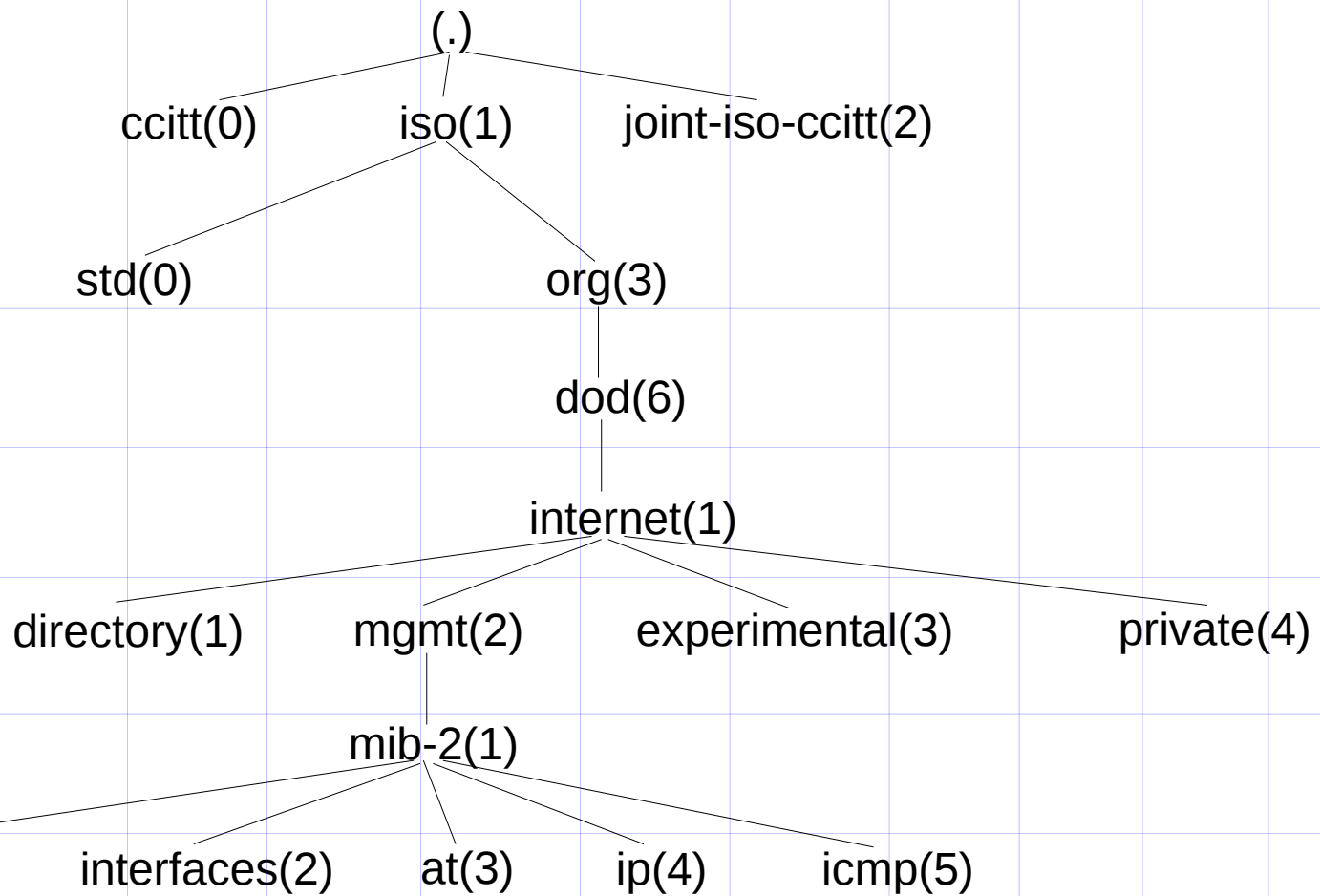


# MIB

## Management Information Base

- hierarchie - stromová struktura
- více standardizačních organizací
  - ISO
  - CCITT (ITU-T )
- objekty
  - skalární
  - tabulka


# MIB



sysDescr(1)

.1.3.6.1.2.1.1

.iso.org.dod.internet.mgmt.mib-2.system.sysDescr



# Monitorovací utility

- lokální systém
  - ifconfig / route / ip
  - arp
  - ipables
  - lsof
  - netstat
  - tcpdump
  - iwconfig / iwlist / iwspy
- testování sítě
  - ping
  - traceroute
  - telnet
  - nmap



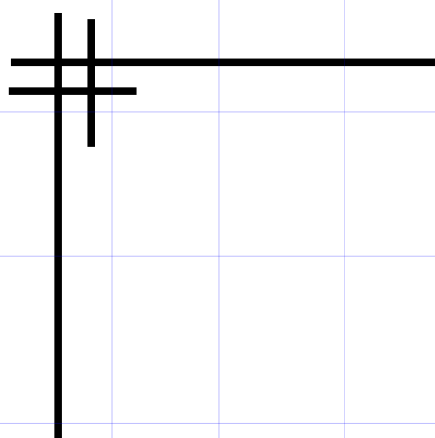
# Síťové rozhraní - Linux

- nástroje Linuxu pro testování síťového rozhraní
  - ifconfig
    - základní nastavení síťového rozhraní (IP adresa, maska, broadcast, MTU, ...)
  - route
    - nastavení statických směrovacích pravidel
  - ip
    - jako ifconfig a ip + další funkce
  - arp
    - zobrazení a manipulace s tabulkou ARP
  - netstat
    - zobrazí síťová spojení, směrovací pravidla, statistické údaje



# Síťové rozhraní (2)

- iptables
  - filtrovací pravidla, NAT, ...
- Isof
  - přehled otevřených síťových spojení
- iwconfig / iwlist / iwspy
  - manipulace s rozhraním WiFi
- tcpdump
  - odchyťávání paketů – filtrovací podmínky



# Nástroje pro testování

- ping
  - využívá ICMP echo\_request
  - zjištění dostupnosti síťového zařízení, měření RTT
- traceroute
  - využívá postupně zvyšující se hodnoty TTL
    - pokud TTL = 0, směrovač pošle zprávu ICMP
  - zobrazí síťové prvky na cestě ke cílovému systému
- telnet
  - klient protokolu *telnet*
  - možnost nastavit cílový port – testování serverů textových protokolů (SMTP, WWW, ....)
- nmap
  - bezpečnostní scanner otevřených portů



Děkuji za pozornost