1. Instalace systému, diskové oddíly, swap, souborový systém, pojem distribuce.

Diskové oddíly(partitions) lze rozdělit na tři základní typy: primární, rozšířené a logické.

- **Primární diskový oddíl**
  - Primární diskový oddíl je takový diskový oddíl, o kterém jsou informace uloženy v MBR (Master Boot Record). Protože MBR je velice malý (512 bytů)- je uložen ve speciální oblasti disku – v prvním sektoru cylindru 0, hlavička 0, která se nazývá tabulka diskových oddílů (partition table), lze vytvořit nejvýše čtyři primární diskové oddíly.
- **Rozšířený diskový oddíl**
  - Rozšířený diskový oddíl je speciálním typem primárního diskového oddílu (z toho plyne, že rozšířený oddíl musí být jedním ze čtyř možných primárních oddílů) obsahujícím další diskové oddíly. Rozšířený diskový oddíl původně neexistoval, ale protože maximální počet čtyř primárních oddílů byl málo, objevilo se toto řešení umožňující rozšíření zaběhlého schéma bez ztráty zpětné kompatibility.
- **Logický diskový oddíl**
  - Logický diskový oddíl je diskový oddíl uvnitř rozšířeného diskového oddílu. Jejich definice není ukládána do MBR (kam by se z principu nevešla), ale je uchovávána v rozšířeném diskovém oddílu. Množství logických diskových oddílů je neomezené.

Proč dělit disk-Většina uživatelů vyčlení pro Linux více než jeden oddíl na disku. Jsou k tomu dva důvody.

- Prvním je **bezpečnost**, pokud dojde **k poškození filesystému**, většinou se to týká pouze jednoho oddílu, takže potom musíte nahradit ze záloh pouze část systému. Jako minimum můžete uvážit vydělení kořenového svazku souborů. Ten obsahuje zásadní komponenty systému. Jestliže dojde poškození nějakého dalšího oddílu, budete schopni spustit Linux a provést nápravu, může Vám to ušetřit novou instalaci systému.
- Druhý důvod je obyčejně závažnější při pracovním nasazení Linuxu, ale záleží k čemu systém používáte. Představte si situaci, kdy nějaký proces začne **nekontrolovaně zabírat diskový prostor.** Pokud se jedná o proces se superuživatelskými právy, může **zaplnit celý disk**. Naruší chod systému, poněvadž Linux potřebuje při běhu vytvářet soubory. K takové situaci může dojít z vnějších příčin, například nevyžádaný e-mail Vám lehce zaplní disk.

Swap – není souborovým systémem, ale prostorem, kam si OS Linux průběžně ukládá běhová data, která se nevejdou do operační paměti. Windows používají obyčejný soubor. Swapuje se na harddisk. swapovat muzete na:

- **partition**
- do **souboru** na filesystemu

Vyhody a nevyhody swapovani jsou u:

- **Partition:**
  - +Je asi 5* rychlejsi nez do souboru
  - +Ze se ma do nej swapovat lze rici jadru jiz pri startu
  - -Kdyz nestaci jeho velikost tak mate holt smulu
- **Souboru:**
  - +Lze ho vytvorit na existujicim filesystemu
  - -Je uzasne pomalej
  - +Kdyz dochazi pamet i vsechny existujici swap zarizeni tak lze vytvorit a pridat dalsi soubor

Souborový systém (*filesystem*) je označení pro způsob organizace informací (ve formě souborů) tak, aby bylo možné je snadně najít a přistupovat k nim. Souborové systémy mohou používat paměťová média jako pevný disk nebo CD, mohou poskytovat přístup k datům uloženým na serveru (síťové souborové systémy, např. NFS, SMB) nebo mohou poskytovat přístup k čistě virtuálním datům (např. **procfs** v Linuxu). Souborový systém umožňuje ukládat data do souborů, které jsou označeny názvy. Obvykle také umožňuje vytvářet adresáře, pomocí kterých lze soubory organizovat do stromové struktury.
žurnálovací souborové systémy patří např. NTFS**, JFS,** HFS+**,** ext3**,** XFS **nebo** ReiserFS**.**

GNU/Linuxová distribuce je označení kompletu programových balíků provozovatelných na operačním systému GNU/Linux. Tzn. nejenom vlastního jádra operačního systému ale i dalších aplikací, které mohou být, ale většinou nejsou autorským dílem distributora.

Tyto distribuce se liší například ve způsobu instalace programových balíků, integrací vlastních konfiguračních metod, atp. V angličtině „*to distribute*“ znamená rozšířit, rozprostřít, rozdat ap.

distribuce

Debian – Tato distribuce je jedna z nejstarších. Je to přísná open-source distribuce, která je vyvíjena dobrovolníky z celého světa. Debian nabízí on-line repozitář (server, kde jsou uloženy zdrojové kódy) softwarových balíků.

Ubuntu – Tato distribuce vhodná pro začátečníky vychází z Debianu. Je volně dostupná, včetně možnosti bezplatného zaslání instalačních CD poštou. Ubuntu zajišťuje komunitní i profesionální podporu. Nové verze vychází dvakrát do roka. Kromě Ubuntu existuje ještě **Kubuntu**, které používá grafické uživatelské rozhraní KDE, nebo **Xubuntu**, které používá grafické uživatelské rozhraní Xfce narozdíl od Ubuntu, které používá GNOME. Také existuje **Edubuntu**, které je zaměřeno na výuku.

2Start počítače, zavaděče OS, jádro, start unixových OS, runlevels.

runlevel

Když počítač bootuje, proces init prohledá konfigurační soubor /etc/inittab a najde, do kterého runlevelu má bootovat. Runlevel je reprezentován číslem od nuly do šesti

Tabulka runlevelů

0 vypnutí systému
1 jednouživatelský režim (všechny služby vypnuté, k dispozici pouze jedna virtuální konzole pracující pod superuživatelem
2 normální režim bez grafického prostředí a síťových služeb
3 normální režim bez grafického prostředí
4 rezervován – například pro vytvoření vlastního runlevelu
5 normální režim
6 restart systému

3Správa a údržba souborových systémů, typy souborových systémů, žurnál, metoda copy-on-write, zálohování.

Linux podporuje širokou škálu souborových systémů. Pro naše účely si je rozdělíme na tři skupiny:
- speciální filesystémy
- "nativní" filesystémy
- filesystémy pro zpětnou kompatibilitu

Nativní filesystémy

EXT2

EXT3
Ext3 přidává k filesystému ext2 podporu **žurnálu**, ale jako takový může být stále namountován jako ext2. Pro uživatele ext2 je navíc zajímavá možnost bezpečného upgradu z ext2 na ext3. Utility pro správu ext2 mohou být také použity pro ext3.

Ext3 je dobrý kompromis mezi stabilitou a funkcemi. Rozumně v něm fungují **ACL**, **žurnál** je poměrně čistě dodělaný a téměř nedegraduje výkon. Výhodou také je, že ho lze **bezpečně zmenšit** a **zvětšit**, a dokonce i zvětšit přimountovaný filesystém. Ext3 je velmi otestovaný a široce podporovaný filesystém, takže pokud nemáte speciální požadavky, bude určitě dobrou volbou.

JFS
JFS byl vytvořen s důrazem na vysokou spolehlivost a rychlost. Postupem času uvolněný pod open source licencí. JFS má **žurnál**, **kvóty** zvládne při použití externího patche, **EA/ACL** v něm nejsou implementovány vůbec, filesystém **může být pouze zvětšen.**

Žurnálovací systém souborů zapisuje změny, které mají být v počítačovém systému souborů provedeny, do **speciálního záznamu nazývaného žurnál**. **Žurnál** je obvykle realizován jako cirkulární buffer a jeho účelem je **ochránit data na pevném disku** před ztrátou integrity v případě neočekávaných havárií (výpadek napájení, neočekávané přerušení vykonávaného programu, pád systému apod.). Žurnál podporují: NTFS, XFS, HFS+, ext3 nebo ReiserFS.

Žurnál je pro ochranu prováděné transakce využíván následujícím způsobem:
1. do žurnálu je zapsáno, co a kde se bude měnit
2. je provedena vlastní série změn
3. do žurnálu je zapsáno, že operace byla úspěšně dokončena
4. záznam v žurnálu je zrušen

Copy-on-write
Princip spočívá v tom, že v okamžiku, kdy je vydán příkaz k pořízení kopie dat, se ve skutečnosti fyzická kopie nevytvoří, a aplikaci je předán toliko jiný odkaz na již existující data. Skutečná kopie je vytvořena teprve ve chvíli, kdy jedna z aplikací sdílejících společnou kopii vydá pokyn k zápisu dat.
ZFS nemá žurnálovací systém, protože integrita dat je dostatečně zajištěna právě technologií Copy-on-write!

4Sdílení dat, síťové souborové systémy, NFS, SMB/CIFS, šifrované souborové systémy.

Síťové souborové systémy (*network filesystem*) je označení pro systémy souborů, které jsou **dostupné prostřednictvím počítačové sítě**. Ve skutečnosti leží soubory a adresáře na jiném počítači a přistupujeme k nim pomocí **speciálních síťových volání služeb** (např. **SMB, NFS**). Na vzdáleném počítači jsou pak soubory a adresáře fyzicky uloženy v podobě klasického systému souborů. Speciálními síťovými systémy souborů jsou **distribuované souborové systémy** (např. GFS v Linuxu), které se mohou rozkládat na několika počítačích, které jsou navzájem propojeny pomocí počítačové sítě.

Server Message Block (SMB) je síťový komunikační protokol aplikační vrstvy, který slouží ke sdílenému přístupu k souborům, tiskárnám, sériovým portům a další komunikaci mezi uzly na síti. Poskytuje také autentizovaný mechanismus pro meziprocesovou komunikaci. Je využíván hlavně na počítačích s operačními systémy rodiny Windows.
Protokol pracuje na principu klient-server. Server umožňuje klientům sítě přistupovat k tzv. sdílenům prostředkům, např. sdíleným disk, adresářům, tiskovým frontám nebo pojmenovaným kanálům.

Network File System (NFS) je internetový protokol pro **vzdálený přístup k souborům přes počítačovou síť**. Protokol byl původně vyvinut společností Sun Microsystems v roce 1984, v současné době má jeho další vývoj na starosti organizace Internet Engineering Task Force (IETF). Funguje především nad transportním protokolem UDP, avšak od verze 3 je možné ho provozovat také nad protokolem TCP.

V praxi si můžete prostřednictvím NFS klienta připojit disk ze vzdáleného serveru a pracovat s ním jako s lokálním. V prostředí Linuxu se jedná asi o nejpoužívanější protokol pro tyto účely.

Programy pro šifrovaní FS

- TrueCrypt
- EncFS

TrueCrypt

TrueCrypt je open source nástroj pro on-the-fly šifrování obsahu dat na disku pro operační systémy Microsoft Windows, Linux a Mac OSx. TrueCrypt umožňuje vytvářet virtuální disky v podobě souboru, který lze snadno připojit a pracovat s ním jako s jakýmkoliv jiným pevným diskem, nebo zašifruje celý diskový oddíl. Soubor má vždy plnou velikost, kterou si zadáme při vytváření, aby případný útočník nezjistil, jaké množství dat máme zašifrováno a uloženo. Od verze 5.0 umí také šifrovat oddíl, ze kterého se bootuje operační systém (toto platí pouze pro verzi Windows). Šifrování a dešifrování probíhá transparentně při zápisu a čtení z disku na pozadí a uživatel se nemusí o nic starat. TrueCrypt podporuje mnoho šifrovacích algoritmů – AES, Blowfish, DES, Triple DES, Twofish a Serpent.

EncFS

EncFS je nástroj, který nám poskytuje šifrovaný FS v uživatelském prostoru. Ke své práci využívá známého jaderného modulu FUSE. Mezi jeho přednosti patří automatická změna velikosti souborového systému tak, jak do něho vkládáme nebo mažem data. Nemusíme dopředu určovat kolik místa si vynahradíme pro své soubory. EncFS je pouze vrstva nad souborovým systémem, proto jej můžeme využít téměř kdekoliv. Pro aplikace je přístup k souborům plně transparentní. EncFS používá algoritmy **AES** nebo **blowfish**, které nám zaručí, že je útočník neprolomí. EncFS je dostupný v mnoha distribucích linuxu, např. v Ubuntu je obsažen balíček deb.

Výhody a nevýhody

Výhody

- Bezpečí dat odcizených a ztracených počítačů
- Zamezení přístupu k datům pro ostatní uživatele
- Ochrana osobních údajů proti útokům zvenčí

Nevýhody

- Při zapomenutí hesla přicházíme o vešjerá data
- Do jisté míry zpolený zápis a čtení z disku

5 Správa uživatelských účtů a skupin, autentizace, PAM, Kerberos, práva, monitorování činnosti uživatelů.

Správa uživatelských účtů a skupin,
Pridani uzivatele do skupiny: **sudo adduser --ingroup root lama**
smazani uzivatele: **sudo deluser --remove-home (--remote-all-files)**
přihlazeni jako uživatel: **su jmeno**
Informace o skupinách jsou uloženy v souboru **/etc/group**
Informace o uživatelech jsou uloženy v souborech **/etc/passwd** a **/etc/shadow**.
Soubor **/etc/passwd** v sobě uchovává kompletní seznam uživatelských **účtů**, a to jak reálných, tak systémových (virtuálních).
Soubor **/etc/shadow** obsahuje zakryptované hesla k jednotlivým účtům.
add group guest student
Pridani skupiny: **addgroup student**
Smazani skupiny: **groupdel skupina**

Práva souborů a adresářů

Práva u souborů

r umožňuje čtení souboru
w umožňuje zápis do souboru
x umožňuje spuštění souboru jako programu

Práva u adresářů
Z předchozího odstavce je patrné, že práva adresářů (s výjimkou práva x) neovlivňují možnost čtení, zápisu a spouštění souborů. Ovlivňují však možnost výpisu obsahu adresáře, vytváření, rušení a přejmenování souborů a podadresářů podle následující tabulky:

r umožňuje vypsat jména souborů a podadresářů v adresáři
w samo o sobě není k ničemu; spolu s právem x umožňuje vytvářet, rušit a přejmenovávat soubory a podadresáře
x umožňuje vypsat informace o souboru nebo podadresáři se známým jménem, Je podmínkou pro všechny operace s obsahem adresáře kromě vypsání jmen

CHMOD Příkaz chmod slouží ke změně práv souboru. První číslice udává práva vlastníka, druhá práva skupiny, třetí ostatních. chmod 751 pictures. Právo r má hodnotu 4, právo w 2, a právo x 1.

hodnota	práva
0	---
1	--x
2	-w-
3	-wx
4	r--
5	r-x
6	rw-
7	rwx

Další možností jako zadávat práva je symbolickým zápisem – práva 751 je možné přidělit zápisem **u=rwx,g=rx,o=x**. Písmena před rovnítkem znamenají

u user vlastník
g group skupina
o others ostatní
a all vlastník, skupina i ostatní

Po spuštění **SUID** programu poběží jeho proces pod právy vlastníka. V případě **SGID** je to obdobné, proces poběží pod právy skupiny.
SUID/SGID byty se přidávají pomocí **`chmod +s`**, **resp.** **`chmod -s`**.
Číselné nastavení:

Právo	**Binární**	**Oktalový**
StickyBit	001	1
SGIDBit	010	2
SUIDBit	100	4

Napište všechny potřebné příkazy, kterými vytvoříte adresář pom, v němž bude moci kdokoli vytvářet soubory, ale **rušit je bude smět pouze jejich vlastník**.
mkdir pom
chmod 222 pom
chmod u+t pom
chown zmena majitele a skupiny

Příkaz **umask** zobrazuje nebo nastavuje implicitní masku práv pro nově vytvářené soubory.
0 rwx
1 rw-
2 r-x
3 r--
4 -wx
5 -w-
6 --x
7 --
umask 027 majitel vsechno skupina zapis ostatni nic
umask 022 majitel vse skupina a ostatni vse

PAM je mechanizmus pro integraci více nízkoúrovňových autentizačních schémat do API, což umožňuje programům opírajícím se o autentizaci uložit uživatelské údaje nezávisle na použitém mechanizmu přihlášení. **PAM**-jednotný systém autentizace.
Díky PAM je možné bez úpravy aplikace užívající PAM měnit autentizační mechanismy, které aplikace používá. Tedy je možné provést upgrade kompletně celého lokálního autentizačního systému bez jakéhokoli zásahu do samotných aplikací. Programy, které potřebují autentizovat uživatele, mohou zavolat funkci z PAM, která projde s uživatelem autentizační proces a vrátí programu výsledek – uživatel prošel/neprošel. Jako příklady programů, kterým se PAM hodí, můžeme uvést login, su, passwd.
PAM je dostupný snad pro všechny UNIXové systémy – Linux, Solaris, IRIX.

Kerberos je síťový autentizační protokol umožňující komukoli komunikujícímu v nezabezpečené síti prokázat bezpečně svoji identitu někomu dalšímu. Kerberos zabraňuje odposlechnutí nebo zopakování takovéto komunikace a zaručuje integritu dat. Byl vytvořen primárně pro model klient-server a poskytuje vzájemnou autentizaci – klient i server si ověří identitu své protistrany. Kerberos je postavený na symetrické kryptografii a potřebuje proto důvěryhodnou třetí stranu.

monitorování činnosti uživatelů

EtherApe – grafický nástroj sloužící k monitorování komunikace na síti. Zobrazuje názvy protokolů a IP adresy nebo DNS názvy systémů, se kterými právě váš počítač komunikuje, jednotlivým protokolům pro přehlednost přiděluje odlišné barvy.

process accounting – jádro umožňuje metodu zaznamenávání příkazů vykonaných v linuxu, běžící, čas cpu, kdo spustil, detailní informace o využívání zdrojů, monitorování, přihlášení a odhlášení, provedené příkazy, časy I/O operaci, CPU.

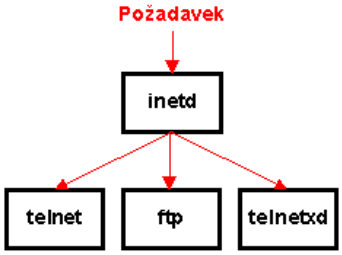
tcpdump – sledování síťového provozu, sledování vytížení sítě, paketů

iptraf-je konzolový program se schopností vytvářet statistické přehledy, které umí i logovat. IPTraf umožňuje monitorovat komunikaci v reálném čase.

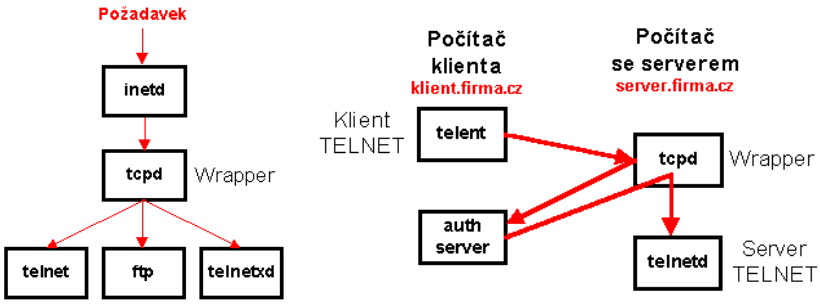
6 Správa síťových služeb, pojem démon, superdémon. Služby, omezování přístupu, aplikační a paketový firewall (tcpd, iptables/ipf), tunelování, VPN.

Jako **démon** se hlavně v unixových počítačových systémech označuje proces, který neustále běží „na pozadí“, kde průběžně vykonává nějakou činnost a není (za běžných okolností) ukončován. Démon obvykle nijak nekomunikuje s uživatelem, pracuje samostatně.

Superdemon inetd Sitovy superdemon. Je vyjimecnym tim, ze se vzbudi kdyz pride nekde ze site pozadavek na urcitou sluzbu, vtedy se vzbudi a spusti taky program alebo demona, ktery konkretnu pozadavku obsluzi. Vyhoda tohto demona je v tom, ze keby nebol, tak by kazda sluzba musela mat demona svojho vlastneho, ktory by ju obsluhoval. Ak vsak mame inetd, vtedy staci iba tento jeden a ten kontroluje vsetky prichodzie poziadavky.



tcpd
Program tcpd je velice užitečným doplňkem našich serverů. Umisťujete-li nějaký server na Internet a nepoužíváte jinou metodu autentizace klientů, pak určitě zvolte alespň program tcpd. **Klient prokazuje svoji totožnost na základě své IP-adresy, případě jména svého počítače**. Tj. **v databázi programu tcpd jsou uvedeny IP-adresy nebo jména počítačů** (případně skupin počítačů) **jimž je přístup povolen**. V případě, že je uvedeno jméno počítače, pak se vezme z příchozího IP-datagramu adresa odesilatele a provede se na ní reverzní překlad DNS. Takto získané jméno se porovnává s databází programu tcpd.



Iptables je nástroj, který umožňuje všeobecně unixovému systému plně pracovat se síťovou komunikací. Pomocí něj si můžeme snadno postavit různé druhy firewallů, nebo sdílení internetu. Vlastně řídí síťovou dopravu na serveru.

- **INPUT** aplikuje pravidla z řetězce na pakety jdoucí dovnitř.
- **OUTPUT** aplikuje pravidla z řetězce na pakety jdoucí ven.
- **FORWARD** aplikuje pravidla z řetězce na pakety jdoucí mezi sítěmi.

sudo iptables -F - vycisteni tabulky
sudo iptables -P INPUT DROP - nastaveni vse zahodit
sudo iptables -A INPUT -p ICMP -j ACCEPT - povoleni ICMP
sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT - povoleni portu TCP/22 (SSH)
sudo iptables -L - vypis pravidel

VPN je prostředek pro propojení několika počítačů na různých místech internetu do jediné virtuální počítačové sítě. I když počítače mohou být v naprosto fyzicky nezávislých sítích na různých místech světa, prostřednictvím virtuální privátní sítě mezi sebou mohou komunikovat, jako by byly na jediném síťovém segmentu.

IP-tuneling znamená, že se vytvoří mezi dvěma body zapouzdřené spojení tzv. tunel. K tunelování je potřeba tunel – kanál pro data mezi dvěma počítači v síti. Tento kanál může být tvořen třeba i TCP spojením, ale v praxi se používá spíše specializovaných protokolů na úrovni IP (**ipsec, gre**).

GRE tunel je obecně typu bod-bod, z toho vyplívá, že pakety v jednom bodě vstoupí do tunelu a vystoupí na druhým konci.

SSH neboli **Secure Shell** je klient/server protokol v síti TCP/IP, který umožňuje bezpečnou komunikaci mezi dvěma počítači pomocí transparentního šifrování přenášených dat.

7 Řízení provozu sítě, omezování rychlosti, policing, shaping a algoritmy (FIFO, TBF, SFQ, RED, PRIO, HTB).

policing, shaping

Nástroje určené k omezování provozu přicházejícího a odcházejícího ze sítě. Příchozí provoz už z principu nejsme moc schopni regulovat. **Policing** se nazývá **zahazování případně pozdržování paketů** nad určitou stanovenou míru. Předpokládáme pak, že odesílatel jich začne posílat méně (TCP).

K **řízení odchozího provozu** použijeme **traffic shaping**. Celé řízení provádíme **pomocí fronty paketů** určených k odeslání, způsob práce s frontou se nazývá **qdisc** (queue discipline). **shaping řeší problém velkého vytížení site**.

Qdisc přiřazujeme jednotlivým rozhraním pakety a dělíme je na třídní a beztřídní (classful, classless). Beztřídní jsou jednodušší a neobsahují další qdiscy.

Díky klasifikaci provozu sítě můžeme nastavit **různým službám různé priority** – např. ssh by mělo mít vyšší prioritu než ostatní síťové služby. Dále můžeme podle různých pravidel **nastavovat minimální (garantované) a maximální rychlosti** různým službám, ale i jednotlivým stanicím na lokální síti. Díky omezování šířky pásma mohou dnešní ISP (Internet Service Provideri) nastavovat svým klientům **různé šířky pásma**, a tím dosáhnout toho, aby jednu **linku sdílelo více uživatelů**, a tím ji efektivně využili.

Fronty paketů

Jednotlivé pakety se před vysíláním nebo po přijetí řádí do fronty. Pakety čekající ve frontě je možné ovlivňovat pomocí disciplín **qdisc** (queue discipline).

Existují dva základní typy disciplín:

- **classless** – dokáže pakety ve výstupní frontě "přeházet", zdržet či zahodit.
- **classful** – omezování spočívá v **rozřazení provozu**, který přichází do výstupní fronty, **do jednotlivých tříd** (class). Mluvíme o klasifikaci provozu. Klasifikace se děje **na základě filtrů**, které jsou definovány uživatelem.

Classless qdisc

- **FIFO** – implicitní fronta, která je automaticky nastavena u classful qdisc. Funguje na principu "kdo první příjde, první odchází". Fronta není tedy moc spravedlivá, a proto je rozdělena na tři menší fronty. Pakety jsou do front řazeny podle příznaku TOS (type of service).
- **TBF** (Token Bucket Filter) – vhodný pro jednoduché omezení rychlosti na síťovém rozhraní. Obsahuje kapsu (buffer), do které si ukládá pakety. Z kapsy postupně odesílá pakety nastavenou rychlostí. Po přetečení kapsy, jsou pakety zahazovány. Ve výsledném efektu je díky kapse TBF fronta odolná vůči menším výpadkům.
- **SFQ** (Stochastic Fairness Queueing) – snaží se pásmo rovnoměrně rozdělovat mezi datové proudy. Algoritmus používá více front, mezi kterými rovnoměrně postupně přepíná. Datové proudy jsou hashovací funkcí rozděleny do jednotlivých front. Hashovací funkce se v průběhu mění, aby nezůstávaly datové proudy dlouho v jedné frontě.

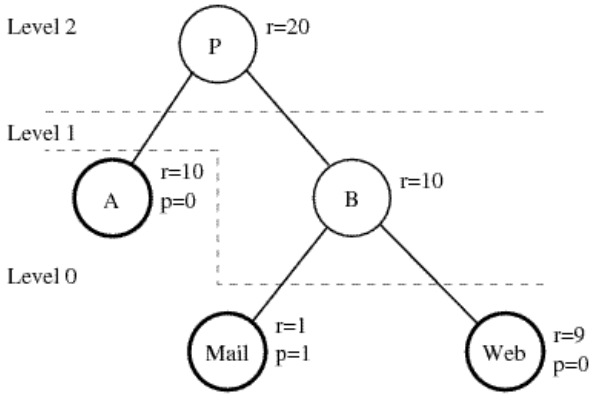
- **RED** (Random Early Detect, Random Early Drop) – určen pro vytížené páteřní spoje. Podle vypočítaných statistik snižuje zátěž zahazováním paketů před zahlcením linky. Čím blíže je celkový traffic maximální hodnotě, tím více jsou pakety zahazovány.

Classful qdisc

- **CBQ** (Class Based Queueing) – dlouho používaná a na nastavení velmi bohatá qdisc. Podporuje libovolné vnořování tříd. Třídy mohou půjčovat svou konektivitu podtřídám a získávat od předků. Podporuje také priority.
- **HTB** (Hierarchical Token Bucket) – obdoba CBQ. Má intuitivnější nastavení a svojí silou pro většinu případů dostačuje. HTB nepoužívá propočty nečinnosti linky jako je tomu u CBQ.
- **PRIO** – podobné na FIFO. Vytvoří 3 třídy, které mají prioriy 0, 1 a 2. Třídy se zpracovávají postupně od nejnižší priority po nejvyšší, ale na rozdíl od FIFO lze na ně pověsit libovolnou jinou qdisc.

Praktické použití HTB

Běžný problém, který administrátoři řeší, je znázorněn na Obrázku 1. Provider P potřebuje rozdělit internetové pásmo mezi firmy označené A a B. Každá firma má specifický požadavek na garantovaný tok *r* a maximální odezvy. Velikost odezvy přitom záleží na prioritě *p* třídy. Firma B si navíc přeje oddělit datové toky pro mailové a webové služby.



Obrázek 1. Sdílení kapacity linky