Ďalšie služby počítačových sietí

Dan Keder keder@fi.muni.cz

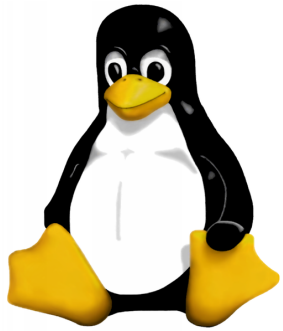
Centrum výpočetní techniky
Fakulta informatiky
Masarykova univerzita

15. október 2008

Obsah

Úvod

- Prehľad rôznych sieťových protokolov a služieb
- Internet nie je len modrá ikonka v tvare písmena 'e', ktorú možno máte na ploche :-)
- Väčšinu prezentovaných vecí si môžete vyskúšať v Linuxe či v inom podobnom systéme



Automatická konfigurácia siete

BOOTP
Bootstrap protocol

- BOOTP – RFC 951, 1533, 1542
- Jednoduchý protokol pre pridelenie IP adresy klientovi
- Bezdiskové stanice, automatické inštalácie OS
- Nutná podpora vo firmware sieťovej karty
- UDP, porty 67 (server) a 68 (klient), správy `BOOTREQUEST` a `BOOTREPLY`

DHCP
Dynamic Host Configuration Protocol

- DHCP – RFC 2131, 3132
- Rozširuje možnosti BOOTP, spätná kompatibilita s BOOTP
- Klientovi umožňuje nastaviť sieťové rozhranie
- Adresy sa prideľujú na základe MAC adresy alebo dynamicky z určitého rozsahu; klientom sa po určitý čas rezervuje naposledy pridelená adresa
- Správy `DHCP Discover`, `Offer`, `Request`, `Acknowledge`, `Release`

Adresárové a autentizačné služby

Adresárové a autentizačné služby

- **Autentizácia** – overenie totožnosti užívateľa
- **Adresárové služby (Directory services)**
  - poskytujú prístup k rôznym informáciám (napr. údaje o užívateľoch)
  - optimalizované pre read-only prístup
- **Autentizačné služby**
  - umožňujú overiť totožnosť užívateľa
  - Dva prístupy: lokálne na každom stroji alebo centralizovane pre mnoho počítačov
- Single Sign-on

BSD flat files

- Lokálne uložené informácie o užívateľoch a skupinách užívateľov
- Formát DSV (delimiter separated values), ľahko prístupné a strojovo spracovateľné
- `/etc/passwd`
  - `login:passwd:uid:gid:gecos:home_dir:shell`
- `/etc/shadow`
  - `login:enc_passwd:a:b:c:d:e:f:reserved`
  - `a-f` – password aging information
  - `enc_passwd` – šifrované heslo (`crypt(5)`, MD5)
- `/etc/group`
  - `name:passwd:gid:members`

LDAP
Lightweight Directory Access Protocol

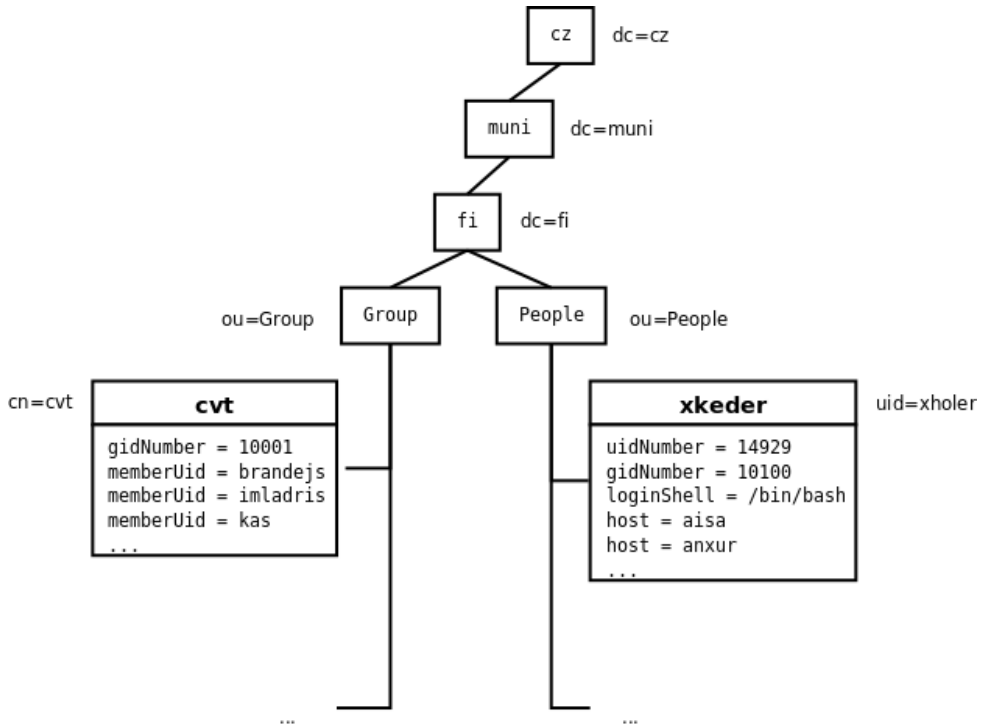
- Centralizovaná adresárová služba
- Vychádza z ISO štandardov X.500, v praxi sa moc nepoužíva, príliš zložité
- LDAP je "odľahčená" verzia protokolu X.500 Directory Access Protocol
- Pôvodne ako brána k X.500, neskôr plnohodnotná služba s mnohými rozšíreniami
  - štandardné API, datové formáty, ...
- Sieťová komunikácia nad TCP/IP
- Výhody: internetový štandard, ľahká integrácia do aplikácií
- Konkrétne implementácie: OpenLDAP, Active Directory (Microsoft), Open Directory (Apple)

- **Directory Information Tree (DIT)** – konkrétny návrh štruktúry stromu
- **Distinguished Name (DN)** – jednoznačne identifikuje položku v globálnom mennom priestore adresárového stromu
- **Relative DN** – jednoznačne identifikuje položku v rámci jednej vetvy stromu

- Schéma má hierarchickú stromovú štruktúru (používa sa DNS)
- Uzly i listy stromu uchovávajú záznamy
  - záznamy sú zložené z atribútov
  - každý záznam má určitý typ (*objectClass*)
  - povinné a voliteľné atribúty
  - záznam môže mať súčasne niekoľko typov
  - príklad atribútov
    - *dc* – domain component
    - *c* – country
    - *o* – organization
    - *ou* – organization unit name
    - *cn* – common name

LDAP
LDAP strom na FI

- `ldap.fi.muni.cz`
- Udržuje informácie o unixových užívateľoch a skupinách (ekvivalent `/etc/passwd` a `/etc/group`)



LDAP
Praktický príklad I.

- Vyskúšajte si na strojoch nymfe:

```
$ ldapsearch -x -H ldap://ldap.fi.muni.cz \
-b ou=People,dc=fi,dc=muni,dc=cz uid=xkeder

$ ldapsearch -x -H ldap://ldap.fi.muni.cz \
-b ou=Group,dc=fi,dc=muni,dc=cz cn=cvt
```

LDAP
Praktický príklad II.

- Výstup vo formáte LDIF (LDAP Data Interchange Format):

```
dn: uid=xkeder,ou=People,dc=fi,dc=muni,dc=cz
uid: xkeder
cn: xkeder
objectClass: account
objectClass: posixAccount
objectClass: shadowAccount
userPassword:: e2NyeXB0fXg=
loginShell: /bin/bash
uidNumber: 14929
gidNumber: 10100
homeDirectory: /home/xkeder
gecos: Daniel Keder
(...)
```

Kerberos

Kerberos

- Centralizovaná autentizačná služba
- RFC 1510, 1964
- Overenie identity bez posielania tajných dát sieťou
- Dve strany (A, B) a dôveryhodný server (KDC, Key Distribution Center)
- A i B zdieľajú s KDC nejaké tajomstvo – heslo
- KDC generuje lístok, zašifruje heslom A a pošle klientovi
- Klient A dešifruje svojím heslom a lístok použije k preukázaniu svojej identity
- Pekný popis algoritmu na `http://en.wikipedia.org/wiki/Kerberos_(protocol)`

- **principal** – užívateľ, stroj alebo služba
- `primary/instance@realm`
  - jedinečná identifikácia užívateľa, služby alebo stroja v databáze Kerbera
  - `primary` – meno užívateľa alebo služby, 'host'
  - `instance` – voliteľná časť v závislosti na `primary` (napr. hostname)
  - `realm` – logická sieť reprezentovaná kerberovskou databázou a KDC (väčšinou zhodná s DNS doménou)
- Napríklad
  - `xkeder@FI.MUNI.CZ`
  - `host/aisa.fi.muni.cz@FI.MUNI.CZ`
  - `ftp/aisa.fi.muni.cz@FI.MUNI.CZ`

Kerberos
Praktický príklad

- Vyskúšajte si na strojoch nymfe:
  - `kinit` – získanie lístku od KDC
  - `klist` – výpis získaných lístkov
  - `kdestroy` – zmazanie získaných lístkov

PAM
Pluggable Authentication Modules

- PAM je sada knižníc integrujúca rôzne autentizačné mechanizmy do jedného API.
- Oddelenie detailov autentizácie od aplikácie, konfigurovateľnosť autentizačného procesu
- Dostupný na väčšine unixových systémov
- Modulárny princíp, je jednoduché zmeniť proces či pridať nový spôsob autentizácie (napr. odtlačky prstov)
- Existuje množstvo modulov, i pre Kerberos, LDAP

- Konfigurácia uložená súboroch v adresári `/etc/pam.d/`
- Každá aplikácia tu má svoj vlastný konfiguračný súbor
- Štyri časti autentizačného procesu:
  - `account` – ako overiť existenciu a platnosť užívateľského účtu
  - `auth` – ako overiť totožnosť užívateľa
  - `password` – ako urobiť zmenu hesla
  - `session` – správa sedenia (napr. auditing)
- Pre každú časť by mal byť nastavený aspoň jeden modul
- Každý modul má nastavenú "dôležitosť" (required, sufficient, optional, requisite)

PAM
Príklad konfigurácie

```
auth        required      pam_env.so
auth        sufficient    pam_thinkfinger.so
auth        sufficient    pam_unix.so \
try_first_pass likeauth nullok
auth        required      pam_deny.so
account     required      pam_unix.so
password    sufficient    pam_unix.so \
try_first_pass use_authtok nullok md5 shadow
password    required      pam_deny.so
session     required      pam_limits.so
session     required      pam_unix.so
```

Vzdialený prístup

SSH
Secure Shell

- RFC 4250 až 4256
- SSH je protokol, ktorý umožňuje bezpečnú komunikáciu v sieti medzi dvoma počítačmi
  - Zabezpečuje **dôvernosť** a **integritu** dát
- Hybridný kryptosystém
  - používa asymetrickú kryptografiu k overeniu totožnosti oboch účastníkov
  - používa symetrickú kryptografiu na šifrovanie prenášaných dát
- Dve verzie:
  - v1: moc sa nepoužíva, známe bezpečnostné chyby
  - v2: používa sa dnes, má čistejšiu architektúru než v1 (spojová, autentizačná a transportná vrstva), podpora silnejších šifier
- Asi najznámejšia implementácia: OpenSSH

- Server počúva na TCP porte 22
- Metódy autentizácie:
  - "password" – jednoduché overenie hesla
  - "publickey" – privátny + verejný kľúč
  - "keyboard-interactive" – server posiela klientovi výzvy na zadanie autentizačných údajov
  - GSSAPI – autentizácia pomocou Kerbera
- Šifrovacie algoritmy:
  - 3DES, RC4, AES, Blowfish, CAST
- Vzájomná dohoda na metóde autentizácie a šifrovacom algoritme

- Umožňujú prihlasovanie na vzdialené počítače "bez hesla"
- Asymetrická kryptografia – privátny a verejný kľúč
- Vytvorenie kľúča:

```
$ ssh-keygen -t dsa
```

- Privátny kľúč uložený väčšinou ako `~/.ssh/id_dsa`, verejný `~/.ssh/id_dsa.pub`
- Zoznam **verejných** kľúčov oprávnených prihlásiť sa v súbore `~/.ssh/authorized_keys`
- Možnosť použiť `ssh-agent(1)` a `ssh-add(1)` k zapamätaniu hesiel SSH kľúčov

SSH
Možnosti použitia

- Primárne navrhnuté ako náhrada za `telnet` a `rsh`
  - spúšťanie procesov na vzdialenom počítači
- Široké možnosti použitia
  - synchronizácia súborov a adresárov (v spolupráci s `rsync`)
  - tunelovanie TCP/IP spojení
  - bezpečný X11-forwarding
  - bezpečné pripojenie vzdialeného adresára na lokálny stroj (`sshfs`)
  - ...

SSH
Praktické príklady

- Triviálny príklad

```
$ ssh user@server.example.com
```

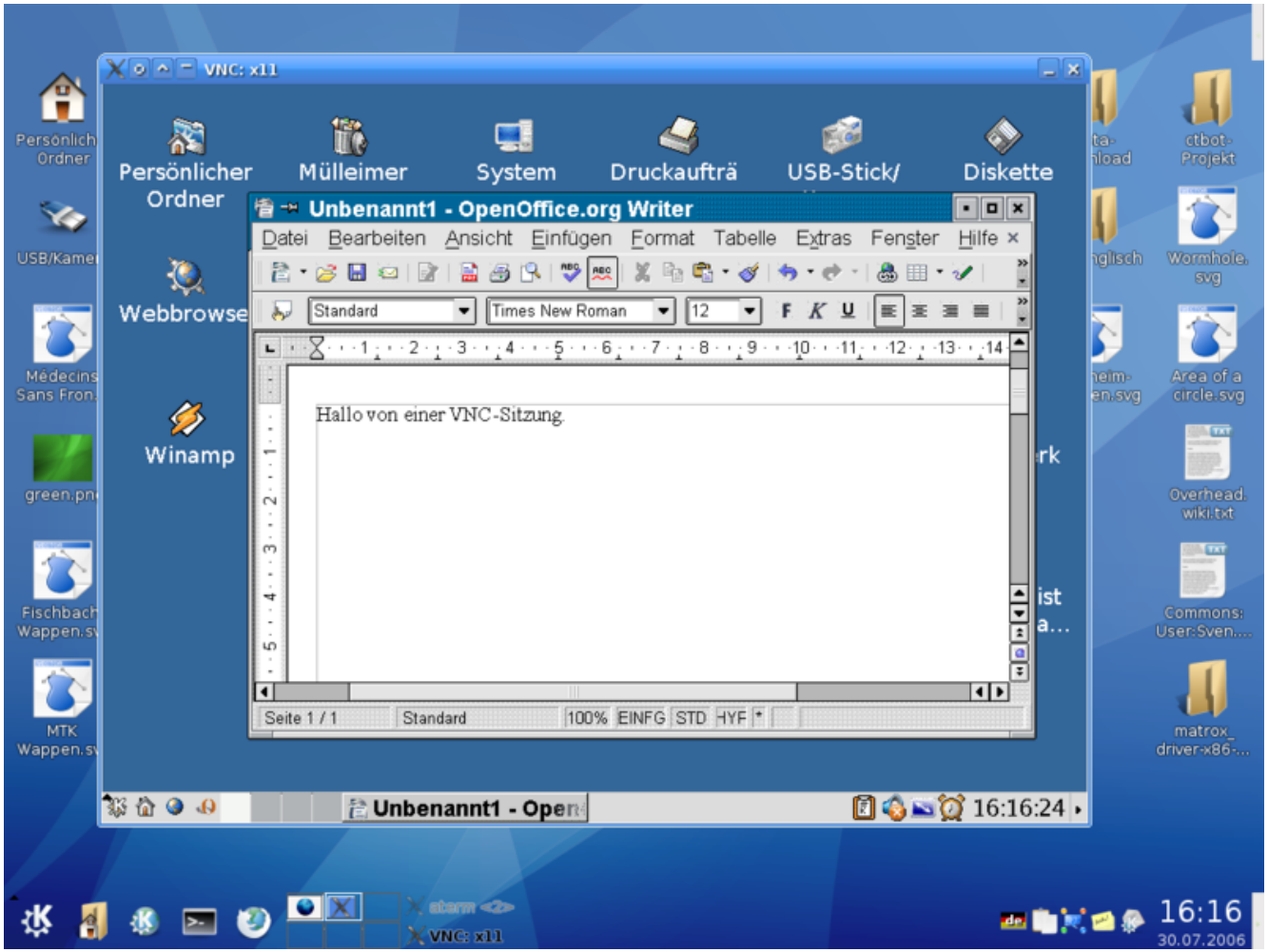
- X11 Forwarding

```
$ ssh -X -f user@server.example.com xclock
```

- Tunelovanie TCP spojení

```
$ ssh -f -L 1234:localhost:6667 \
    server.example.com sleep 10
$ irc -c '#users' -p 1234 pinky localhost
```

VNC
Virtual Network Computing I.



VNC
Virtual Network Computing II.

- Umožňuje vzdialené ovládanie počítača
  - "Vzdialená pracovná plocha"
- Platformne nezávislé
- Dve súčasti
  - server – periodicky posiela klientovi časti obrazovky, ktoré sa zmenili (ako bitmapu)
  - klient (viewer) – zobrazuje u užívateľa pracovnú plochu vzdialeného počítača, zasiela serveru udalosti (myš, klávesnica)
- Efektívny prenos prenášaných dát – podpora rôznych kódovaní

VNC
Virtual Network Computing III.

- TCP porty 5900 – 5906
- Nezabezpečený protokol, tunelovanie cez SSH
- Použitie
  - náhrada X11 forwardingu – lepší výkon v pomalej sieti
  - virtualizácia – prístup na bežiaci virtuálny stroj
  - možnosť pripojiť sa k existujúcemu X11 sedeniu (x11vnc)
  - ...
- Implementácie: x11vnc, tightvnc, Apple Remote Desktop

Zdieľanie súborov v sieti

FTP
File Transfer Protocol

- Protokol pre prenos súborov nad TCP
- Riadiaci kanál (port 21), dátový kanál (port 20)
- Dva režimy prenosu dát:
  - aktívny – *klient* serveru oznámy neprivilegovaný port, na ktorom počúva, server otvorí dátové spojenie
  - pasívny – *server* klientovi oznámi neprivilegovaný port, na ktorom počúva, klient sám otvorí dátové spojenie
- Problémy
  - chýbajúce šifrovanie (hlavne hesiel a dát)
  - samostatné dátové spojenie pre každý prenos
  - aktívny režim nefunguje za NAT (Network Address Translation)

SCP
Secure Copy Protocol

- Prenos súboru medzi dvoma stanicami cez SSH
- Klient komunikuje so vzdialene spusteným `scp`
- Obmedzenia
  - max. 4GB súbory
  - nepodporuje obnovenie prenosu
  - nedá sa vypísať obsah adresára
  - podpora kompresie dát (vhodné pre pomalé linky)
- Triviálny príklad:

```
$ scp test.txt user@server.example.com
```

SFTP
SSH File Transfer Protocol

- Podobné vlastnosti ako SCP, bez vypísaných obmedzení
- Nemá nič spoločného s protokolom FTP
- Od základu novo navrhnutý, používaný v SSHv2 (ako jeho subsystém)
- Užitočný program pre MS Windows: WinSCP

NFS
Network File System

- Protokol sprístupňujúci po sieti vzdialené zväzky
- Niekoľko generácií:
  - v1: experimentálny
  - v2: pôvodne bezstavový protokol nad UDP s podporou zámkov; neskôr dopracovaná podpora TCP
  - v3: vyšší výkon, súbory $> 4GB$; málo bezpečné, ale **rýchle**
  - v4: vyšší výkon, väčsia bezpečnosť (šifrovanie, autentizácia), internetový štandard

CIFS
Common Internet File System

- Pôvodne protokol SMB (Server Message Block) od IBM, značne prepracovaný Microsoftom.
- Nielen zdieľanie súborov, ale i zdrojov (tlačiarne)
- Pôvod vo Windows, existujú i otvorené implementácie pre iné operačné systémy
- Horšia implementácia vo Windows, často zneužívané chyby
- Výkonovo horšie než NFS

Synchronizácia času

Synchronizácia času

- Prečo synchronizovať čas
  - potreba presného času nie je až tak dôležitá
  - dôležitá je predstava o súvislosti dejov
  - je dôležité mať všade **rovnaký** čas
- Možné riešenia:
  - vzájomná dohoda uzlov na čase
  - časový synchronizačný server so (sprostredkovaným) presným časom
- Protokoly na synchronizáciu času: Time, Daytime, NTP

NTP
Network Time Protocol

- RFC 778, 891, 956, 958, 1305
- Protokol prenosu aktuálneho času cez médium s premenlivou dobou doručenia informácie
- UDP port 123
- Časové servery hierarchicky radené
  - stratum 0 – atómové hodiny a pod., veľká presnosť
  - stratum 1 – synchronizované so stratum 0
  - stratum 2 a 3 – synchronizácia koncových počítačov
  - (. . .) – teoreticky až 256 úrovní

NTP
Network Time Protocol

- Čas uplynutý od 1.1.1900 00:00 uložený v 64bitovej hodnote
  - 32b počet sekúnd
  - 32b desatinná časť
- Pre korekciu času používa Marzullov algoritmus
- Podpora vo Windows i unixových systémoch
- Synchronizujte si svoj čas podľa `time.fi.muni.cz` :-)

Záver
Kde hľadať podrobnejšie informácie

- Repozitár RFC dokumentov
  - `http://tools.ietf.org/html/`
- Manuálové stránky a oficiálna dokumentácia k programom
- Google, Wikipedia :-)

Záver

Koniec