

Servery v počítačových sítích

Luboš Matějka
KIV
FAV ZČU Plzeň

Téma přednášky

- **Nastavení sítě**
 - Statické, DHCP
- **DNS**
 - Princip, typy záznamů, typy serverů, registrace
- **WWW**
 - Implementace, programovací jazyky, web clustery
- **E-mail**
 - MTA, MDA, MUA, směrování, spam
- **Umístění serverů a aplikací**
 - Webhosting, ServerHosting

Nastavení konektivity

- Statické

- Bezpečné
- Pro malý počet stanic
- Problém při rekonfiguraci
- Příklad nastavení pro Linuxový server :

```
auto eth0
```

```
iface eth0 inet static
```

```
    address 147.228.63.10
```

```
    netmask 255.255.255.0
```

```
    network 147.228.63.0
```

```
    broadcast 147.228.63.255
```

```
    gateway 147.228.63.1
```

```
    dns-nameservers 147.228.52.11
```

```
    dns-search fav.zcu.cz
```

Nastavení konektivity

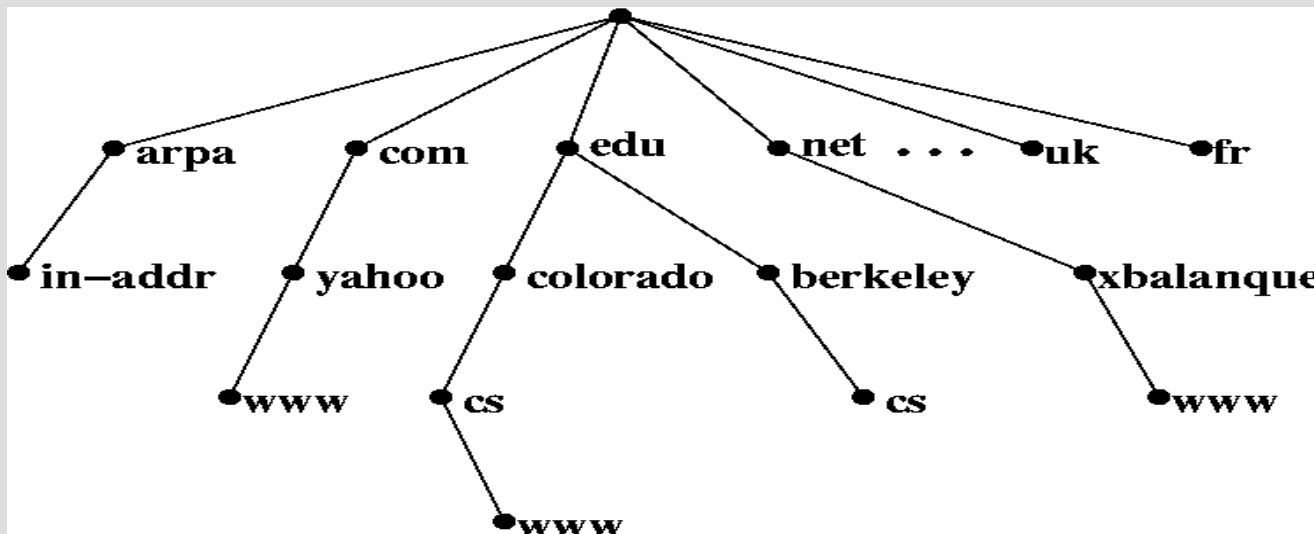
- Dynamické
 - DHCP
 - Dočasné přidělování adres – cca 600s
 - Fixace pevných adres pro zařízení -tiskárny
 - Vhodné pro větší sítě
 - Přiřazování podle MAC adres
 - Funguje v rámci broadcastové domény
 - DHCP Relay Agent
 - Více DHCP serverů v síti == problém
 - IP, maska sítě, brána, DNS servery, doména
 - Bezdiskové stanice

Nastavení konektivity

```
option domain-name "fav.zcu.cz";
option domain-name-servers 147.228.52.11;
default-lease-time 600;
max-lease-time 7200;
subnet 147.228.63.0 netmask 255.255.255.0 {
    range 147.228.63.5 147.228.63.250;
    option routers 147.228.63.1;
}
host notebook {
    hardware ethernet 00:1e:a4:ac:48:42;
    fixed-address 147.228.63.10;
}
```

DNS

- Mapování IP adres na jména a opačně
 `www.kiv.zcu.cz -> 147.228.63.11`
 `147.228.63.11 -> proteus.fav.zcu.cz`
- TCP/UDP porty 53
- Stromová struktura



DNS Kořenové servery

- Decentralizovaný systém
- 13 kořenových serverů



DNS Typy záznamů

Záznamy

- A IPv4 adresa
- AAAA IPv6 adresa
- CNAME alias na A
- MX mail exchange + priorita
- NS nameserver
- PTR reverzní záznam pro IP

- Omezení
 - Max 63 znaků v jedné úrovni
 - Max délka 255 znaků
 - Max 127 úrovní stromu

DNS Typy serverů

- **Primární server**
 - Udržuje informace o zónách
 - Autoritativní odpovědi
- **Sekundární server**
 - Informace o zónách přejímá od primárního serveru
- **Pomocný - cachovací server**
 - Dočasně udržuje informace
 - Zrychluje reakce sítí
 - Problém při nedodržení TTL
 - Neautoritativní odpovědi
- **Běžné implementace**
 - Bind, DJBDNS, MyDNS

DNS Registrace domén

- Registrace u správce nadřazené domény
- 41 samostatných registrátorů
 - Různé ceny
 - Různá rozhraní
 - Různá rychlost
 - Ignum, Active24, Forpsi,
- Nutné dva DNS servery
 - Glue pro dns servery ve vlastní doméně
 - Například pro ahoj.cz ns1.ahoj.cz
- Dvouúrovňová expirace
 - 0-30 dnů – registrovaná a v aktivní
 - 30-45 dnů - registrovaná a neaktivní

DNS Zabezpečení, Ověření

- DNSSEC
 - Ověření platnosti záznamu
 - Zabezpečení klíčem
 - Expirace zabezpečení
 - Částečně podporované registrátory
- Ověřování domén
 - ping, nslookup, dig
 - whois
 - <http://www.lupa.cz/nastroje/whois/>

WWW

- Nejběžnější služba v internetu
- Vznik v roce 1990
- TCP 80 a 443
- Protokol http
 - Původně bezstavový
 - Následně rozšířen o cookie
 - Původně jen pro HTML, nyní přenáší libovolná data
 - Základní příkazy :
 - GET, HEAD, POST, PUT, DELETE, CONNECT, TRACE, OPTIONS

WWW Zabezpečení

- HTTPS – šifrované http (TCP/443)
- Pro přenos citlivých dat
- Vytváří šifrovaný tunel pro přenos HTTP
- Každý HTTPS virtual vlastní IP
- Nutný certifikát
 - Vlastní pomocí openssl zdarma, neznají jej klienti
 - Vystavený certifikační autoritou, placený, důvěryhodný
 - Thawte, Verisign
 - Cena od 2500Kč na rok

WWW – Nedůvěryhodný certifikát



Existuje problém s certifikátem zabezpečení tohoto webu.

Certifikát zabezpečení předložený tímto webem nebyl vydán důvěryhodným certifikačním úřadem.

Problémy s certifikátem zabezpečení by mohly ukazovat na pokus podvést vás nebo zachytávat data, která odešlete na server.

Doporučujeme, abyste zavřeli tuto webovou stránku a nepokračovali na tento web.

 Tuto webovou stránku zavřete kliknutím sem.

 Pokračovat na tento web (nedoporučujeme)

 Další informace

WWW Konfigurace

- Dostupná řešení pro Windows, Linux ...
 - Apache, Lighttpd, tHttpd, Boa, Tomcat, Winstone
- Jeden server obsluhuje více domén
- Doména musí být nastavena před spuštěním serveru

```
<VirtualHost *:80>
    ServerName students.kiv.zcu.cz
    ServerAlias students.fav.zcu.cz
    ServerAdmin webmaster@mail.kiv.zcu.cz
    DocumentRoot /home/www/apache/students.kiv.zcu.cz
    ErrorLog /var/log/apache2/students-error.log
    CustomLog /var/log/apache2/students-access.log
    Alias /vs/ /home/validator/vs2/data/html/
</VirtualHost>
```

WWW a HTML

- Původně prosté HTML
- Postupně rozšiřované o programovací jazyky
 - Na straně klienta JavaScript
 - Na straně serveru CGI, PHP, ASP, Java, Python, Perl...
 - Kombinace AJAX, typicky pro našeptávače
 - Často kombinované s databázemi
 - MySQL, PostgreSQL, Oracle, MS SQL
 - Bezpečnostní problémy
 - Neošetřená vstupní data
 - Spouštění programů na serveru
 - Spam

WWW Cluster

- Webové servery v clusteru
- Round robin
 - Založeno na DNS s více A či CNAME záznamy
 - Nereaguje na zátěž ani výpadek
- Balancer
 - Softwarový
 - Pound, Squid, apache+proxy modul
 - Speciální HW
 - F5, Cisco
 - Failover i balancer
 - Rozklad na základě více parametrů
 - Load, Browser, dostupnost

WWW cluster



E-mail

- Druhá nejběžnější služba na internetu
- Decentralizované jako DNS
- Těsně svázané s DNS
- Tři části
 - MUA Mail User Agent
 - MTA Mail Transport Agent
 - MDA Mail Delivery Agent

E-mail MUA

- Mailový klient
- Ovládá stahování i odesílání pošty
- Komunikuje na více portech i protokolech
- GUI aplikace
 - Outlook, Outlook Express, Thunderbird, Evolution
- Webové aplikace
 - Horde, Squirrelmail, Gmail, Yahoo, Seznam
- Konzolové aplikace
 - Mutt, Pine, Telnet

E-mail MUA Mutt

```
ssh
Mutt 1.2.5i: =lug (threads) [156/156] [N=0,*=0,post=0,new=0]
 74  F 19.07 09:44 To LUG-FFM          ( 0.6K) ^->Re: LUG: FTP Problem
 75  r F 18.07 22:29 To LUG-FFM          ( 1.2K) LUG: DHCP
-> 76  F 18.07 23:31 To LUG-FFM          ( 0.7K) ^->
 77  r   19.07 01:49 helmex            ( 0.3K) LUG: libc.so.6 futsch
 78   19.07 09:38 Stephan.Goll@t-on    ( 1.1K) |*>
 79   19.07 16:02 helmex            ( 1.2K) | |->
 80   19.07 16:16 Andreas Spengler    ( 0.6K) | | ^->
- [76/F] Christoph Rummel (22) Re: LUG: DHCP -- (79%)
From lug-ffm-owner@informatik.uni-frankfurt.de  Wed Jul 18 23:34:01 2001
X-Authentication-Warning: hera.rbi.informatik.uni-frankfurt.de: majordom set
+sender to owner-lug-ffm@informatik.uni-frankfurt.de using -f
Date: Wed, 18 Jul 2001 23:31:19 +0200
From: Christoph Rummel <bronski>
To: LUG-FFM <lug-ffm@informatik.uni-frankfurt.de>
Subject: Re: LUG: DHCP
User-Agent: Mutt/1.2.5i
In-Reply-To: <20010718222939.V415708@arago.de>; from "Christoph Rummel" on
+2001-07-18 22:29:39 +0200
Precedence: bulk
Reply-To: lug-ffm@informatik.uni-frankfurt.de

Christoph Rummel <bronski>:
> Und dann Win2000... Nichts! Nada! Nix! Gerade davon
> haette ich eigentlich erwartet, dass es auf Anhieb
> funktioniert!

Du kriegst die Motten... *seufz*

Jul 18 23:22:55 6D:ohm dhcpd: DHCPDISCOVER from 00:d0:59:3e:21:b0 via ef0
Jul 18 23:22:55 6D:ohm dhcpd: DHCPOFFER on 10.0.0.24 to 00:d0:59:3e:21:b0 via
+ef0

Zu bloed das zu nehmen, was einem angeboten wird!
Windows weigert sich schlichtweg, oder ist taub! Dummes
Stueck Software!

Weiter am suchen...
i:Exit ^B:PrevPg ^F:NextPg v:View Attachm. d:Del ,a:Reply ,j:Next ?:Help
```

E-mail Stahování pošty

- Většinou klient stahuje poštu ze serveru
- POP3/POP3S
 - Starší a jednodušší řešení
 - Stahuje pouze celé maily
 - Komunikuje na TCP/110, TCP/995
- IMAP/IMAPS
 - Umožňuje stahovat jen hlavičky mailů
 - Umožňuje filtrovat maily před stažením
 - Komunikuje na TCP/143, TCP/220, TCP/993
 - Více zatěžuje server indexací
 - Umožňuje synchronizovat schránky mezi více stroji

E-mail MTA

- Mailový server
- Komunikace na TCP/25 případně TCP/465
- Přijímá poštu od MUA a předává dalším MTA či MDA
- Směřuje poštu na základě
 - MX záznamů – směrování podle domén
 - A záznamů – směrování podle stroje
 - Vlastních tabulek - statické směrování
- Běžné implementace
 - MS Exchange, Postfix, Sendmail, Kerio Mailsever

E-mail MDA

- Doručování posty do schránek
- Základní MDA umí každý server
- Většinou obsahuje skriptovací jazyk
 - Posílání notifikací o mailech, přeposílání, filtrace
- Rourová řešení
 - Procmail, maildrop
- Síťová řešení
 - LMTP – cyrus
- Integrovaná
 - MS Exchange, Kerio Mailserver

E-mail MDA Maildrop

```
logfile "/var/log/maildrop-filter-log"

#SpamTest
    xfilter "/usr/bin/spamc -d 89.185.231.140"
#Virscan
xfilter "/usr/local/bin/clamassassin"

#SPAM
if( ( /^X-Spam-Status: Yes.* / ) || ( /^X-Virus-
Status: Yes.* / ) )
{
    to "/mail/LOGNAME/Maildir/.spam"
}

# Doruceni podle maildiru
DEFAULT = "/var/mail/$LOGNAME/Maildir"
```

E-mail Nebezpečí

- Není nijak zajištěno, že email dorazí!!!
- Není jisté kdo email poslal
 - Viry
 - Vir lze jednoznačně identifikovat
 - Email je možné smazat či odstranit přílohu
 - Clamav, Node32
 - Spamy
 - Nelze jednoznačně identifikovat, pouze se značkuje
 - Reklama, poplašné zprávy, zaplnění schránek
 - Co je pro jednoho spam pro druhého není :(
 - Spamassassin, blacklisty
 - Open Relay
 - Servery umožňující odesílat poštu komukoliv
 - Šíření spamů a virů,
 - Existují databáze takových serverů

Webhosting

- Umístění aplikace na servery třetích stran
- Operační systémy MS Windows a Linux
- Volba podle jazyku aplikace
 - Linux – PHP, Perl, Java, CGI
 - Windows – ASP, ASP.NET, Java
- Různé principy účtování
 - Zabrané místo, počty účtů, databázi
- Zálohování !!
- Různá Cena
 - Banán, Pípní, Active24, Ignum, ...

ServerHosting

- Umístění vlastního serveru
- Základní požadované parametry
 - Konektivita
 - Klimatizace
 - Technik na místě a vzdálená pomoc
 - Vzdálená konzole a vzdálené ovládání napájení
 - Více zdrojů elektřiny – okruhy x diesel
 - Různá cena
 - GTS
 - Sitel, Internet Master
 - Casablanca, CoolHousing, SuperHosting,

ServerHosting 10 let zpět



ServerHousing Dnes



Děkuji Vám za pozornost

Vaše Dotazy ???