Curs 3
DHCP și SSH

Gestiunea serviciilor de rețea (GSR)
20 octombrie 2016

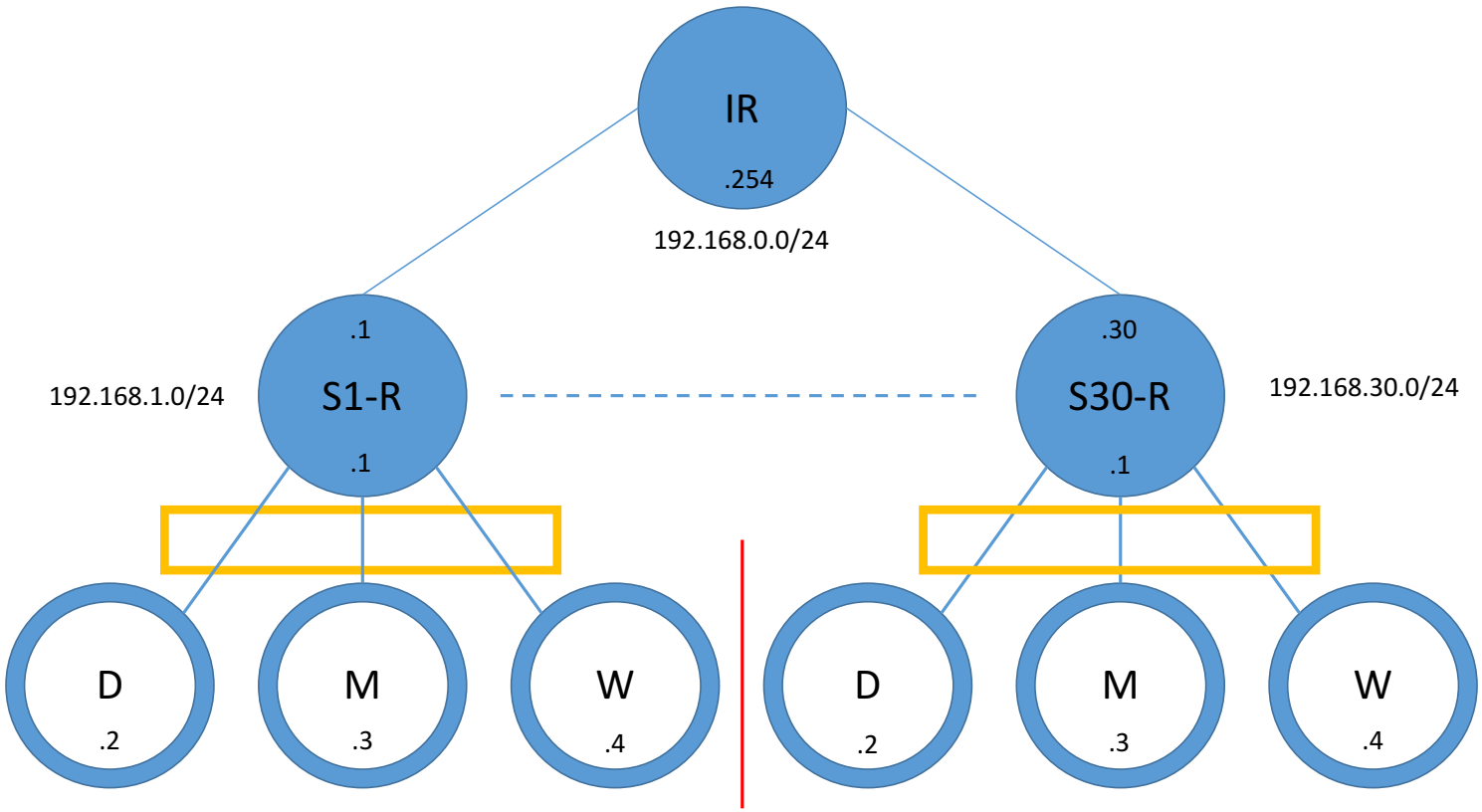
Departamentul de Calculatoare, Comunitatea RLUG

Cuprins

Detalii despre proiect

- Finalitate: Presupune crearea unei rețele de mici dimensiuni, și configurarea unui set de servicii
- Punctaj: 2.5 puncte din nota finală
- Evaluare: în două etape:
  - mid-term, pe 26 noiembrie
  - end-term, în sesiune
- Vom folosi o topologie virtualizată, pe clusterul facultății (necesita autentificare cu contul de pe cs.curs.pub.ro)

Topologia proiectului



Cuprins

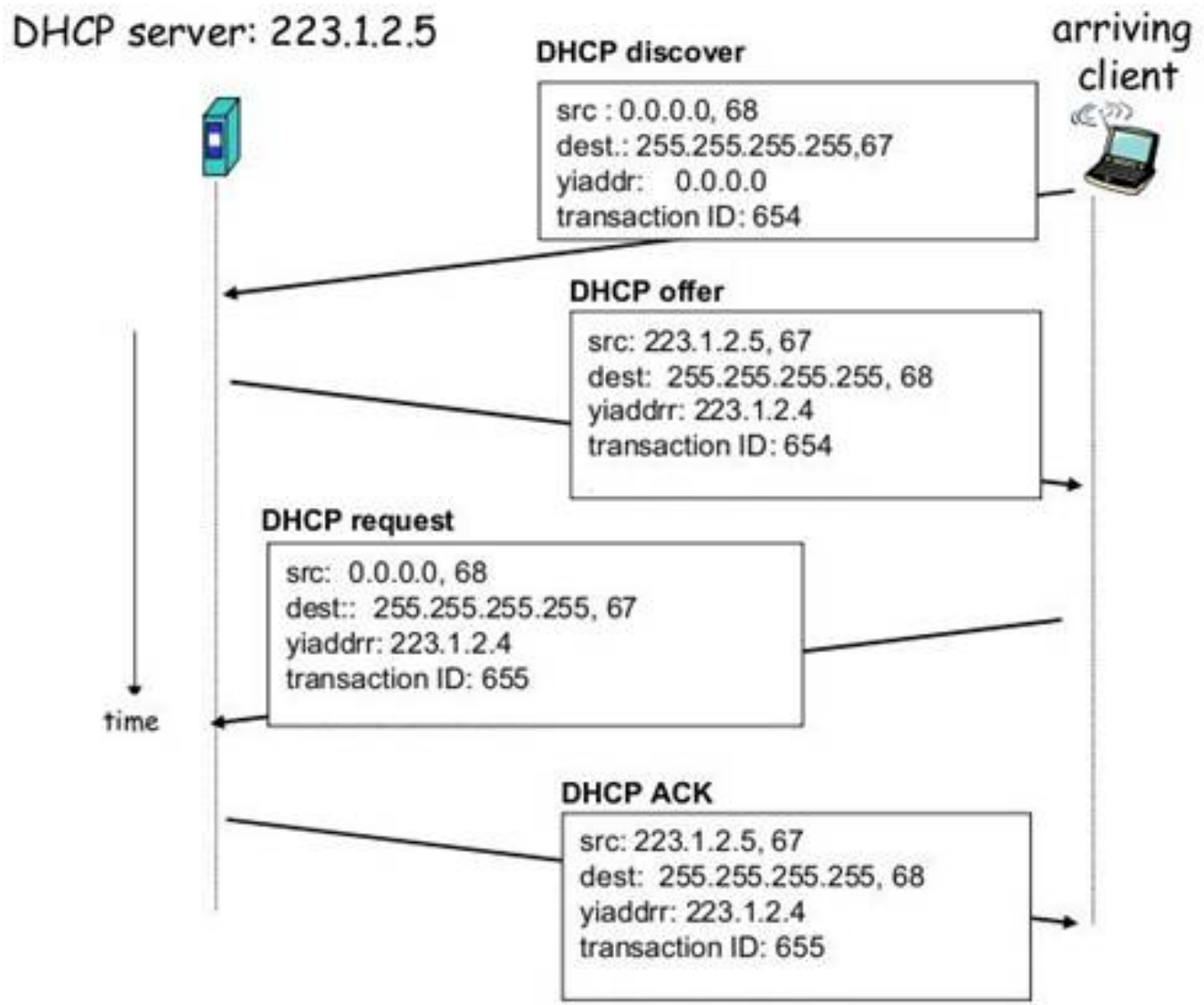
Dynamic Host Configuration Protocol

- Ce este DHCP
- Cum funcționează DHCP
- Cum se configurează ISC `dhcpd`
- Modalități de utilizare

Ce este DHCP

- DHCP este un protocol care:
  - Alocă în mod dinamic adrese IP într-o rețea
  - Transmite parametri de configurare stațiilor din rețea
    - Router (default gateway)
    - DNS Server
    - NTP Server
    - Domain name
    - MTU
    - ...

Cum funcționează DHCP



ISC dhcpd

/etc/dhcp/dhcpd.conf

```
subnet 10.254.239.0 netmask 255.255.255.0 {
  range 10.254.239.10 10.254.239.21;
  option routers 10.254.239.1;
  option domain-name-servers 8.8.8.8;
  option domain-name "my.domain";
  default-lease-time 600;
  max-lease-time 7200;
  host my-special-host {
    hardware ethernet 08:00:07:26:c0:a5;
    fixed-address 10.254.239.11;
  }
}
```

Cuprins

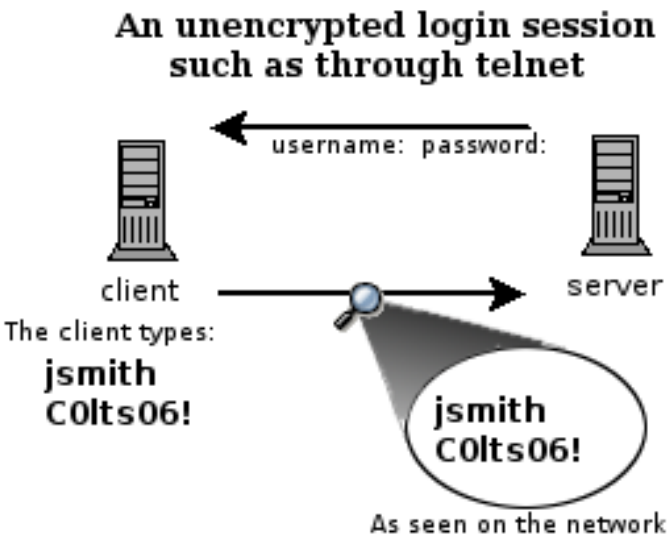
Aducere aminte despre protocolul SSH

- `http://ocw.cs.pub.ro/courses/rl/courses/07`

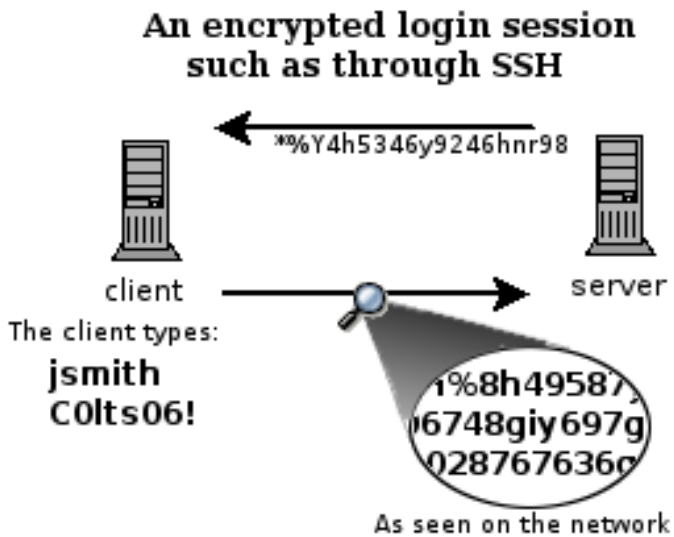
OpenSSH — acces securizat la distanță

- Deși sunt suficient de multe variante de a accesa o consolă de la distanță, SSH este una dintre cele mai populare soluții.
- Una dintre metodele trecute era să folosim aplicația `telnet` disponibilă pe majoritatea sistemelor de operare ce dispun de acces la rețea.
- Diferența dintre Telnet și SSH se traduce în primul rând prin securitatea datelor. Prin Telnet datele sunt transmise în clar, iar prin SSH ele sunt criptate. Este puțin probabil ca un atacator să poată intercepta datele transmise prin SSH, atâta timp cât configurația acestuia respectă bunele practici de securitate.
- Telnet este folosit și în ziua de astăzi pentru administrarea echipamentelor de rețea. Deși acestea suportă SSH/TLS(HTTPS), majoritatea folosesc în mod implicit Telnet.

OpenSSH — transmisie în clar versus transmisie criptată



Datele transmise printr-un protocol necriptat



Datele transmise printr-un protocol criptat

OpenSSH — configurații utile

- `/etc/ssh/sshd_config`
- `PermitRootLogin no`
- `PasswordAuthentication yes`

OpenSSH host key

- Algoritmi: RSA, ECDSA, ED25519
- DSA nu mai este considerat un algoritm sigur
- ED25519 — `https://ed25519.cr.yp.to`

Autentificare cu parolă

- `sshd` poate citi direct `/etc/passwd` și `/etc/shadow`
- `sshd` se integreaza cu `PAM` pentru autentificarea utilizatorilor
- folosind `PAM` se poate integra cu mecanisme de autentificare centralizată
  - `RADIUS`
  - `LDAP`

Autentificare pe bază de chei publice

- Cheile publice folosite de utilizatori pot fi de tipul:
  `dsa` | `ecdsa` | `ed25519` | `rsa`
- Perechile de chei se generează folosind utilitarul `ssh-keygen`
  - `~/.ssh/id_ed25519` — partea privată
  - `~/.ssh/id_ed25519.pub` — partea publică
- `~/.ssh/authorized_keys` — fișierul pe mașina destinație unde se pune cheia publică a utilizatorului

Demo

- `scp` înseamnă "secure copy"
- folosește subsistemul SSH pentru a copia in mod sigur de pe o mașină pe alta fișiere sau directoare
  - `scp user@remotehost:~/foobar.txt .`
  - `scp foobar.txt user@remotehost:~`

Tunele SSH

- Sunt folosite pentru tunelarea traficului TCP de pe client pe mașina de la distanță

Stabilirea unui tunel SSH

```
ssh -L localport:host:hostport user@server -N
```

Demo

Resurse utile

- https://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol
- https://en.wikipedia.org/wiki/Secure_Shell
- https://en.wikipedia.org/wiki/Secure_copy
- http://www.revsys.com/writings/quicktips/ssh-tunnel.html
- http://www.linuxhorizon.ro/ssh-tunnel.html
- https://code.facebook.com/posts/365787980419535/scalable-and-secure-access-with-ssh/