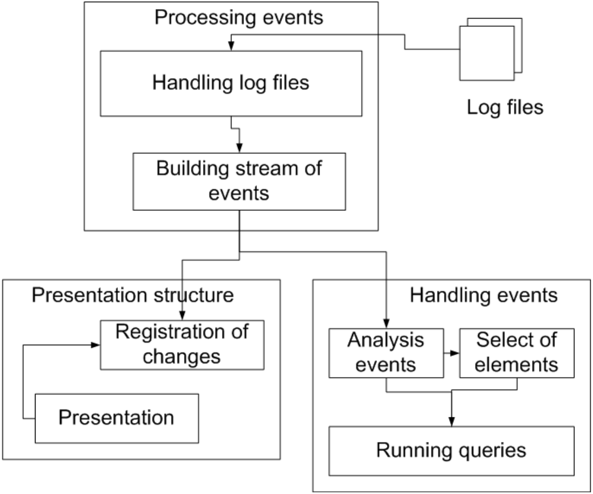
Analysis of DHCP Log Files for Registration of Different Events in Network

Vyacheslav Dimitrov   Yury A. Bogoyavlenskiy

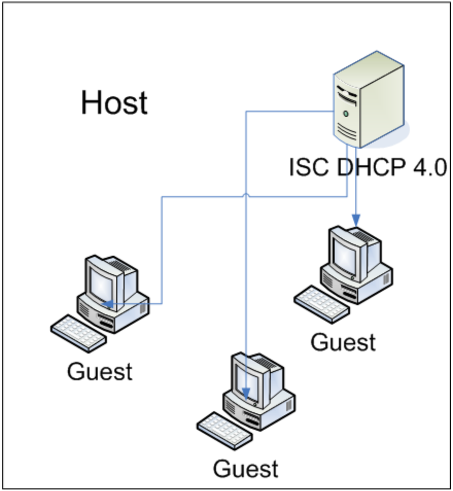
Department of Computer Science
Petrozavodsk State University

Advances in Methods of Information and Communication Technology, 2008

Nest architecture of processing of events



Work's organization



List Events

- PC‘s registration in the net
- Correct work completion of PC in the net
- Incorrect work completion of PC in the net
- Attempt of unknown or forbidden PC to appear in the net
- Lack of IP-addresses which are given out by the DHCP-server

PC‘s registration in the net

The server gives out one of its free IP-addresses and fixed it in its log file:

```
lease 192.168.95.77 {
        starts 0 2008/02/17 17:18:47;
        ends 0 2008/02/17 17:48:47;
        binding state active;
        next binding state free;
        hardware ethernet 00:0c:29:fe:6e:11;
    }
```

Correct work completion of PC in the net

This record we can identify by the mark "binding state":

```
lease 192.168.95.77 {
        starts 0 2008/02/20 23:18:18;
        ends 0 2008/02/20 23:21:59;
        binding state free;
        hardware ethernet 00:0c:29:fe:6e:11;
    }
```

Incorrect work completion of PC in the net

Algorithm:

- Next record with defined MAC.
- If exist two record pc's registration with this MAC, so fix incorrect work completion.
- If doesn't exist update record, so fix incorrect work completion.
- Go to step 1.

Attempt of unknown or forbidden PC to appear in the net

In syslog system the significative record about the try of connection will be fixes:

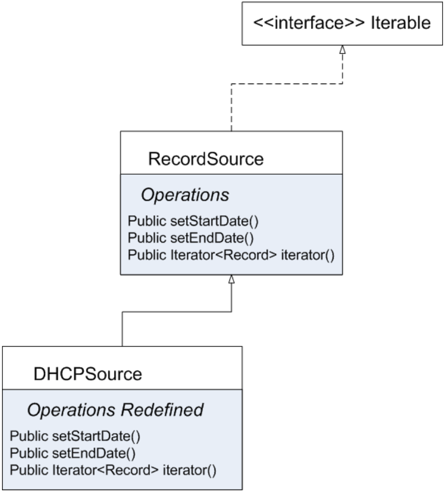
```
Feb 21 19:36:41 aphina dhcpd: DHCPDISCOVER from
00:0c:29:fe:6e:11 via vmnet1: unknown client
```

Lack of IP-addresses which are given out by the DHCP-server

If we have a fixed addresses' range which the server is able to give out but we suddenly have more clients so this situation is fixed in the syslog system:

```
Mar 20 15:56:54 aphina dhcpd: DHCPDISCOVER from 00:0c:29:f7:f2:09 via vmnet1: network 192.168.92.0/24: no free leases
```

Classes for processing sources



<<interface>> Iterable

RecordSource

Operations

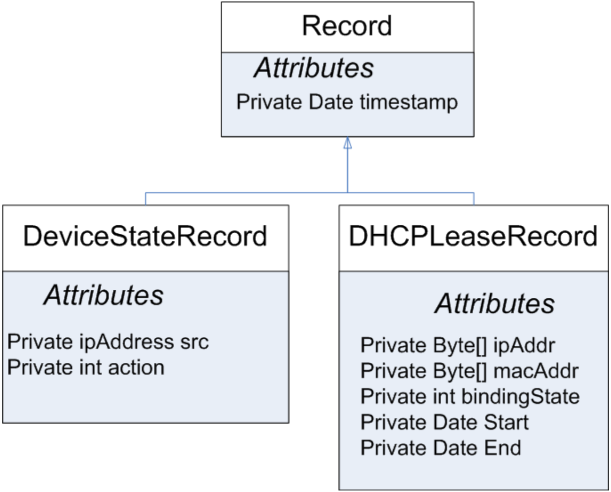
Public setStartDate()
Public setEndDate()
Public Iterator<Record> iterator()

DHCPSource

Operations Redefined

Public setStartDate()
Public setEndDate()
Public Iterator<Record> iterator()

Classes events



Record

Attributes

Private Date timestamp

DeviceStateRecord

Attributes

Private ipAddress src
Private int action

DHCPLeaseRecord

Attributes

Private Byte[] ipAddr
Private Byte[] macAddr
Private int bindingState
Private Date Start
Private Date End

Conclusion

- The work of the report DHCP is investigated
- The events in the net which can be registered on basis of DHCP are discovered
- The Java classes of the DHCP events processing are realized

Thank you for attention!