Tutorial worksheet 10
What you have done so far.

- You have so far configured
  - VLANs
  - Routing protocols within the backbone network (RIP, OSPF, BGP).
  - Wireless mesh networking.
  - IPv6
  - Firewall policies on Linux.
- And now ‘Core Network Operations, monitoring and management.’
Work Load Generation and Monitoring.

- 
- To test network we need to generate traffic with similar characteristics that we see in the real internet. This is called representative web workload.
But how does Web traffic look like
Web traffic generation-Tools

• Iperf
• SURGE
• Harpoon:
  – A Flow-level Traffic Generator by ‘Joel Sommers’
Harpoon Traffic Generator

• The design objectives of Harpoon are
  – to scalably generate application-independent network traffic at the IP flow level
  – to be easily parameterized to create traffic that is statistically identical to traffic measured at a given vantage point in the Internet.
Harpoon usage
Parameters

- File size distributions at server side
- Inter-connection time distributions at client side.
- Other factors (see worksheet 10)
NETFLOW

• A Tool to get aggregated information from routers regarding volume of traffic.
• Cisco uses five tuple flow
  – Source ip
  – Source port
  – Destination ip
  – Destination port
  – Protocol
NETFLOW

• TCP Flows
  – Unidirectional.
  – One TCP connection has two flows.
  – They are exported on every FIN or RST

• UDP flows
  – Exported after some time.
Basic Setup

Web-Client
Requests from clients

Responses from servers

Web-Server

Traffic Measured at Cisco Router has same characteristics as in real internet

Switch

Switch

Netflow on Cisco Router

Flow-Collector
Analysis of Netflow data

- Use linux utility *flow-tools*
- Flow-tools utilities
  - flow-capture
  - flow-report
NetFlow v5 Packet Example

IP/UDP packet

NetFlow v5 header

v5 record

...

...

v5 record
### flow-print

- Formatted output of flow files.

```markdown
\texttt{engl:\% flow-print < ft-v05.2002-01-21.093345-0500 | head -15}

<table>
<thead>
<tr>
<th>srcIP</th>
<th>dstIP</th>
<th>prot</th>
<th>srcPort</th>
<th>dstPort</th>
<th>octets</th>
<th>packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>131.238.205.199</td>
<td>194.210.13.1</td>
<td>6</td>
<td>6346</td>
<td>40355</td>
<td>221</td>
<td>5</td>
</tr>
<tr>
<td>192.5.110.20</td>
<td>128.195.186.5</td>
<td>17</td>
<td>57040</td>
<td>33468</td>
<td>40</td>
<td>1</td>
</tr>
<tr>
<td>128.146.1.7</td>
<td>194.85.127.69</td>
<td>17</td>
<td>53</td>
<td>53</td>
<td>64</td>
<td>1</td>
</tr>
<tr>
<td>193.170.62.114</td>
<td>132.235.156.242</td>
<td>6</td>
<td>1453</td>
<td>1214</td>
<td>192</td>
<td>4</td>
</tr>
<tr>
<td>134.243.5.160</td>
<td>192.129.25.10</td>
<td>6</td>
<td>80</td>
<td>3360</td>
<td>654</td>
<td>7</td>
</tr>
<tr>
<td>132.235.156.242</td>
<td>193.170.62.114</td>
<td>6</td>
<td>1214</td>
<td>1453</td>
<td>160</td>
<td>4</td>
</tr>
<tr>
<td>130.206.43.51</td>
<td>130.101.99.107</td>
<td>6</td>
<td>3226</td>
<td>80</td>
<td>96</td>
<td>2</td>
</tr>
<tr>
<td>206.244.141.3</td>
<td>128.163.62.17</td>
<td>6</td>
<td>35593</td>
<td>80</td>
<td>739</td>
<td>10</td>
</tr>
<tr>
<td>206.244.141.3</td>
<td>128.163.62.17</td>
<td>6</td>
<td>35594</td>
<td>80</td>
<td>577</td>
<td>6</td>
</tr>
<tr>
<td>212.33.84.160</td>
<td>132.235.152.47</td>
<td>6</td>
<td>1447</td>
<td>1214</td>
<td>192</td>
<td>4</td>
</tr>
<tr>
<td>132.235.157.187</td>
<td>164.58.150.166</td>
<td>6</td>
<td>1214</td>
<td>56938</td>
<td>81</td>
<td>2</td>
</tr>
<tr>
<td>129.1.246.97</td>
<td>152.94.20.214</td>
<td>6</td>
<td>4541</td>
<td>6346</td>
<td>912</td>
<td>10</td>
</tr>
<tr>
<td>132.235.152.47</td>
<td>212.33.84.160</td>
<td>6</td>
<td>1214</td>
<td>1447</td>
<td>160</td>
<td>4</td>
</tr>
<tr>
<td>130.237.131.52</td>
<td>130.101.9.20</td>
<td>6</td>
<td>1246</td>
<td>80</td>
<td>902</td>
<td>15</td>
</tr>
</tbody>
</table>
```
SNMP

• Simple Network Management Protocol
  – Runs on UDP
  – client-server
  – Participants
    • 1 manger/Management Station (e.g. router/switch)
    • management agents
SMNP

- Operations: get, set, (trap), (traversal)
- Security: By a simple shared secret (community)
- SNMP MIB
  - MIB: Management Information Base
  - Groups the managed objects into hierarchal namespace.
  - Individual objects addressed via OID (Object Identifier)
SNMP Packet

- Is called PDU (protocol data unit)
- Contains: command, Request ID, Error status, variables
Tools

- snmpget: query a specific object variable
- snmpset: set a specific object variable
- snmpwalk: hierarchically list MIB sub tree