WQL: Distributed Query Processing for Real-time Views using Echo

- Non-trivial application of distributed polling with result aggregation: *dynamic creation of management views for large networks*
  - expressiveness of relational model
  - distributed processing and aggregation of device-level data
- Benefits compared to a centralized management system
  - Scalability--capacity $O(N)$; response time $O(d)$; processing load evenly distributed
  - Robustness---all management nodes perform identical functions
- More information: [Lim Stadler IM05], [Adam Lim Stadler 05]
### Top 25 Flows by Bit Rate

<table>
<thead>
<tr>
<th>Src IP</th>
<th>Dest IP</th>
<th>Src Port</th>
<th>Dest Port</th>
<th>TOS</th>
<th>Application</th>
<th>Bitrate (kbps)</th>
<th>Packet Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.234</td>
<td>192.168.32.167</td>
<td>2132</td>
<td>80</td>
<td>0</td>
<td>http</td>
<td>279.0</td>
<td>44.4</td>
</tr>
<tr>
<td>192.168.4.220</td>
<td>192.168.34.140</td>
<td>424</td>
<td>80</td>
<td>0</td>
<td>http</td>
<td>200.4</td>
<td>31.9</td>
</tr>
<tr>
<td>192.168.3.43</td>
<td>192.168.12.220</td>
<td>1041</td>
<td>389</td>
<td>0</td>
<td>ldap</td>
<td>196.2</td>
<td>31.2</td>
</tr>
<tr>
<td>192.168.3.127</td>
<td>192.168.52.226</td>
<td>2908</td>
<td>389</td>
<td>0</td>
<td>ldap</td>
<td>152.3</td>
<td>25.8</td>
</tr>
<tr>
<td>192.168.3.76</td>
<td>192.168.32.134</td>
<td>381</td>
<td>389</td>
<td>0</td>
<td>ldap</td>
<td>100.2</td>
<td>15.9</td>
</tr>
<tr>
<td>192.168.3.25</td>
<td>192.168.2.93</td>
<td>901</td>
<td>69</td>
<td>0</td>
<td>tftp</td>
<td>100.2</td>
<td>15.9</td>
</tr>
<tr>
<td>192.168.3.163</td>
<td>192.168.13.48</td>
<td>639</td>
<td>69</td>
<td>0</td>
<td>tftp</td>
<td>100.2</td>
<td>15.9</td>
</tr>
<tr>
<td>192.168.3.23</td>
<td>192.168.4.169</td>
<td>1234</td>
<td>194</td>
<td>0</td>
<td>irc</td>
<td>90.2</td>
<td>14.3</td>
</tr>
<tr>
<td>192.168.3.82</td>
<td>192.168.13.60</td>
<td>270</td>
<td>80</td>
<td>0</td>
<td>http</td>
<td>86.2</td>
<td>13.7</td>
</tr>
<tr>
<td>192.168.3.194</td>
<td>192.168.2.36</td>
<td>840</td>
<td>194</td>
<td>0</td>
<td>irc</td>
<td>70.1</td>
<td>11.2</td>
</tr>
<tr>
<td>192.168.1.86</td>
<td>192.168.34.72</td>
<td>2940</td>
<td>25</td>
<td>0</td>
<td>smtp</td>
<td>40.1</td>
<td>6.4</td>
</tr>
<tr>
<td>192.168.1.175</td>
<td>192.168.33.37</td>
<td>1723</td>
<td>25</td>
<td>0</td>
<td>smtp</td>
<td>38.7</td>
<td>6.1</td>
</tr>
<tr>
<td>192.168.4.234</td>
<td>192.168.34.178</td>
<td>13</td>
<td>194</td>
<td>0</td>
<td>irc</td>
<td>30.1</td>
<td>4.8</td>
</tr>
<tr>
<td>192.168.4.233</td>
<td>192.168.32.183</td>
<td>1939</td>
<td>25</td>
<td>0</td>
<td>smtp</td>
<td>30.1</td>
<td>4.8</td>
</tr>
<tr>
<td>192.168.3.170</td>
<td>192.168.16.11</td>
<td>2976</td>
<td>23</td>
<td>0</td>
<td>telnet</td>
<td>23.4</td>
<td>4.5</td>
</tr>
<tr>
<td>192.168.1.224</td>
<td>192.168.32.111</td>
<td>3188</td>
<td>25</td>
<td>0</td>
<td>smtp</td>
<td>9.5</td>
<td>1.5</td>
</tr>
<tr>
<td>192.168.32.2</td>
<td>192.168.5.5</td>
<td>1366</td>
<td>1028</td>
<td>0</td>
<td>other</td>
<td>3.7</td>
<td>1.9</td>
</tr>
</tbody>
</table>
Query: select Application, Sum(ByteCount) as ByteCount, Sum(PacketCount) as PacketCount from Flows where Timestamp > 2004-05-25 11:06:02 group ByteCount desc

<table>
<thead>
<tr>
<th>Application</th>
<th>Byte Count</th>
<th>Packet Count</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>ldap</td>
<td>342.7 K</td>
<td>436.5</td>
<td>(42.6%)</td>
</tr>
<tr>
<td>tftp</td>
<td>172.1 K</td>
<td>219.5</td>
<td>(21.4%)</td>
</tr>
<tr>
<td>irc</td>
<td>152.5 K</td>
<td>193.4</td>
<td>(18.9%)</td>
</tr>
<tr>
<td>http</td>
<td>90.4 K</td>
<td>114.9</td>
<td>(11.2%)</td>
</tr>
<tr>
<td>smtp</td>
<td>27.5 K</td>
<td>34.5</td>
<td>(3.4%)</td>
</tr>
<tr>
<td>telnet</td>
<td>11.8 K</td>
<td>14.9</td>
<td>(1.5%)</td>
</tr>
<tr>
<td>other</td>
<td>8.0 K</td>
<td>40.7</td>
<td>(1.0%)</td>
</tr>
</tbody>
</table>
Local Tables on a Management Node

### System table
- WANIP
- Memory
- FreeDisk
- UpSince

### Device table
- DeviceIp
- NumInterfaces
- Make
- Model
- UpSince

### Interface table
- InterfaceNum
- InterfaceAddress
- InterfaceSubnet
- InterfaceType
- InterfaceSpeed

### Flow table
- SrcIp
- DstIp
- SrcPort
- DstPort
- Application
- ByteCount
- PacketCount
- Protocol
- Timestamp
- SamplingInterval

**WAN data**

**Router data**
The Weaver Query Language WQL

- Queries are expressed in WQL, an extension to SQL
  Extensions refer to scoping, aggregate functions, implicit attributes

```
SELECT <columns>
  FROM <tables>
  [ ON <startnode> [ FOR <hops> ]] 
  [ WHERE <conditions> ]
  [ GROUP BY <groups> [ HAVING <having> ]] 
  [ ORDER BY <ordering> ] [ LIMIT <limit> ]
```

- Queries are executed against virtual global tables
  System table, Device table, Interface table, Flow table
- MIB objects can be accessed via a virtual MIB table.
Identify the heaviest flows currently in the network

```
SELECT MAX(ByteCount*8/SamplingInterval) as BitRate, SrcIp, DstIp, DstPort
FROM Flow
GROUP BY SrcIp, DstIp, DstPort
WHERE Timestamp >= "15:23:00" and Timestamp <= "15:26:00"
ORDER BY BitRate DESCENDING
LIMIT 3
```

<table>
<thead>
<tr>
<th>BitRate</th>
<th>SrcIp</th>
<th>DstIp</th>
<th>DstPort</th>
</tr>
</thead>
<tbody>
<tr>
<td>1245232</td>
<td>192.168.1.45</td>
<td>192.168.2.27</td>
<td>1400</td>
</tr>
<tr>
<td>1212442</td>
<td>192.168.2.56</td>
<td>192.168.3.42</td>
<td>5000</td>
</tr>
<tr>
<td>1022451</td>
<td>192.168.3.17</td>
<td>192.168.51.24</td>
<td>138</td>
</tr>
</tbody>
</table>
### Identify all FTP flows currently traversing two given routers

```
SELECT    SrcIp, DstIp, SET_CONCAT(DeviceIp) as PathSet
FROM      Flow, Device
WHERE     Timestamp >= "15:23:00" and Timestamp <= "15:23:05"
          and Application = "FTP"
GROUP BY  SrcIp, DstIp
HAVING    STRSTR(PathSet,"192.168.1.1") and STRSTR(PathSet, "192.168.4.1")
```

<table>
<thead>
<tr>
<th>SrcIp</th>
<th>DstIp</th>
<th>PathSet</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.24</td>
<td>192.168.4.47</td>
<td>192.168.1.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>192.168.2.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>192.168.4.1</td>
</tr>
<tr>
<td>192.168.21.24</td>
<td>192.168.6.21</td>
<td>192.168.21.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>192.168.4.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>192.168.1.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>192.168.6.1</td>
</tr>
</tbody>
</table>
Mapping a Global Query into Local Queries

**G:**
Global Query

**S1:**
Executed against local databases

**S2:**
Aggregates partial results along spanning tree

```
SELECT MAX((ByteCount*8)/SamplingInterval) 
as BitRate, SrcIp, DstIP
FROM Flow
GROUP BY SrcIp, DstIp
WHERE Timestamp >= "15:23:00" and Timestamp <= "15:26:00"
and Application = "FTP"
ORDER BY BitRate DESCENDING
LIMIT 3
```

```
SELECT SrcIp, DstIp, DstPort, MAX(BitRate) as BitRate
FROM TEMP_TABLE
GROUP BY SrcIp, DstIp
ORDER BY BitRate DESCENDING
LIMIT 3
```

```
CREATE TEMP_TABLE
SELECT MAX((ByteCount*8)/SamplingInterval) 
as BitRate, SrcIp, DstIp
FROM Flow
WHERE Timestamp >= "15:23:00" and Timestamp <= "15:26:00"
and Application = "FTP"
GROUP BY SrcIp, DstIp
ORDER BY BitRate DESCENDING
LIMIT 3
```
Echo Pattern (expansion)

G

S1, S2
Implementation on the Lab Testbed

- 16 Cisco 2600 series routers
- 16 Intrinsyc CerfCubes + Linux 2.4.18+MySQL4.0
The Performance of a WQL Query

- Determining factors
  - Performance of echo patterns [LS01]
    - Execution time: $O(d)$, $d$ is network diameter
    - Message complexity: 2 messages per link
  - Performance of DBMS on WANs
    - Execution time: $T = \alpha ls$
      where
      $\alpha$: constant
      $l$: record length
      $s$: records in local database
  - Network conditions

![Graph showing time in seconds vs. number of records accessed]
Modeling and Validating the Execution time of a WQL Query on Weaver

Upper bound on execution time:

\[ C_{time} \leq d(\frac{\bar{c}}{a} t_q + \alpha s + \gamma t_n + 2 t_n) + 2\alpha U (d - 1) \]

where

- \( d \): diameter of network
- \( s \): records in local database
- \( U \): max records of local S1,S2
- \( a \): DBMS processing capacity

For supremum queries:

\( C_{time} \) proportional to \( \alpha s d \)


