Figure 1: Structure of the Bro system
Dialog

Typing paves way for *dialog* to negotiate communication properties

- (All) Private types
- No Readable types
- No Modifiable types
- *Fewer* private types
- Exe readable
- No modifiable types

Desired level of visibility/control?

Pre-connection or in-band

Sender may choose an alternate path.
Fail if no such path → *reason in full view*

Network has upper hand, but visibility limits collateral damage
Progression of Communication

1. Route discovery
2. Policy discovery
3. Path selection
4. Key exchange
5. Encrypted typed transfer
6. Message reception
It is also worth noting that the flow table can be several orders-of-magnitude smaller than the forwarding table in an equivalent Ethernet switch. In an Ethernet switch, the table is sized to minimize broadcast traffic: as switches flood during learning, this can swamp links and makes the network less secure.\textsuperscript{5} As a result, an Ethernet switch needs to remember all the addresses it’s likely to encounter; even small wiring closet switches typically contain a million entries. Ethane Switches, on the other hand, can have much smaller two-way hashing scheme [9]. A typical commercial enterprise Ethernet switch today holds 1 million Ethernet addresses (6MB, but larger if hashing is used), 1 million IP addresses (4MB of TCAM),

<table>
<thead>
<tr>
<th>Table 1. Scalability Table</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
</tr>
<tr>
<td>MAC Entries</td>
</tr>
<tr>
<td>Routes</td>
</tr>
</tbody>
</table>
Figure 6: Flow-setup times as a function of Controller load. Packet sizes were 64B, 128B and 256B, evenly distributed.
heads. The Controller was configured with a policy file of 50 rules and 100 registered principles; routes were precalculated and cached. Under these conditions, the system could handle 650,845 bind events per second and 16,972,600 permission checks per second. The
Figure 7: Active flows for LBL network [19].

Figure 8: Flow-request rate for Stanford network.