



max planck institut  
informatik

# Automated Reasoning SS06

Uwe Waldmann, Christoph Weidenbach

# Applications

- SUDOKU
- LAN Analysis



# SUDOKU



max planck institut  
informatik

9  
5

|   |   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|---|
|   |   |   |   |   |   |   |   |   |
| 4 |   |   |   |   |   |   |   | 1 |
|   | 2 |   |   |   |   |   |   |   |
|   |   |   | 5 |   | 4 |   |   | 7 |
|   |   |   |   |   |   | 3 |   |   |
|   |   |   |   |   |   |   |   |   |
|   |   | 8 |   |   |   |   |   |   |
|   |   | 1 |   | 9 |   |   |   |   |
| 3 |   |   |   |   | 4 |   | 2 |   |
|   | 5 |   |   |   | 7 |   |   |   |
|   |   |   |   |   |   |   |   |   |
|   |   |   |   |   |   |   |   |   |
|   |   |   |   |   |   |   | 6 |   |
|   |   |   |   |   | 8 |   |   |   |

2, 3, 4

1, 4, 6, 8



# SUDOKU



max planck institut  
informatik

|   |   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|---|
| 6 | 9 | 3 | 7 | 8 | 4 | 5 | 1 | 2 |
| 4 | 8 | 7 | 5 | 1 | 2 | 9 | 3 | 6 |
| 1 | 2 | 5 | 9 | 6 | 3 | 8 | 7 | 4 |
| 9 | 3 | 2 | 6 | 5 | 1 | 4 | 8 | 7 |
| 5 | 6 | 8 | 2 | 4 | 7 | 3 | 9 | 1 |
| 7 | 4 | 1 | 3 | 9 | 8 | 6 | 2 | 5 |
| 3 | 1 | 9 | 4 | 7 | 5 | 2 | 6 | 8 |
| 8 | 5 | 6 | 1 | 2 | 9 | 7 | 4 | 3 |
| 2 | 7 | 4 | 8 | 3 | 6 | 1 | 5 | 9 |



# SUDOKU



|   |   |   |   |          |  |   |  |   |   |
|---|---|---|---|----------|--|---|--|---|---|
|   |   |   |   |          |  |   |  | 1 |   |
| 4 |   |   |   |          |  |   |  |   |   |
|   | 2 |   |   |          |  |   |  |   |   |
|   |   |   |   | 5        |  | 4 |  |   | 7 |
|   |   |   | 8 |          |  | 3 |  |   |   |
|   |   | 1 |   | 9        |  |   |  |   |   |
| 3 |   | 4 |   | <b>7</b> |  | 2 |  |   |   |
|   | 5 |   |   | 1        |  |   |  |   |   |
|   |   |   |   | 8        |  | 6 |  |   |   |

$$\begin{aligned}
 A(8,1) &\approx 1 \wedge A(1,2) \approx 4 \wedge \dots \wedge A(6,9) \approx 6 \\
 A(9,1) &\approx 9 \vee A(9,1) \approx 8 \vee \dots \vee A(9,1) \approx 1 \\
 A(8,1) &\approx 9 \vee A(8,1) \approx 8 \vee \dots \vee A(8,1) \approx 1 \\
 &\vdots \\
 A(1,1) &\approx 9 \vee A(1,1) \approx 8 \vee \dots \vee A(1,1) \approx 1 \\
 A(9,1) &\not\approx A(8,1) \wedge \dots \wedge A(9,1) \not\approx A(1,1) \\
 A(8,1) &\not\approx A(7,1) \wedge \dots \wedge A(8,1) \not\approx A(1,1) \\
 &\vdots \\
 A(2,1) &\not\approx A(1,1)
 \end{aligned}$$

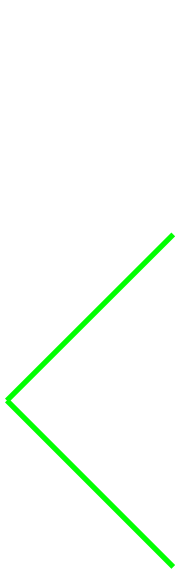
$$\begin{aligned}
 A(5,7) \not\approx A(1,7) &\xrightarrow{\quad} A(1,7) \approx 3 && A(5,7) \not\approx 3 \\
 A(5,7) \approx 9 \vee \dots \vee A(5,7) \approx 3 \vee \dots \vee A(5,7) \approx 1 &&& \\
 &\vdots && \\
 &&& A(5,7) \approx 7
 \end{aligned}$$



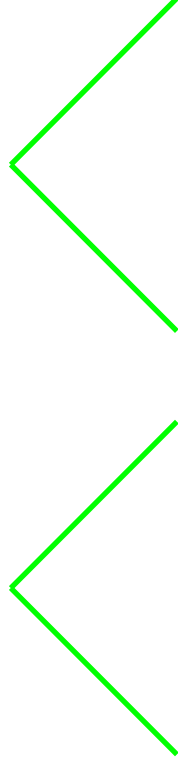
# SUDOKU

|   |   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|---|
| 1 |   |   |   |   |   |   | 1 |   |
| 2 | 4 |   |   |   |   |   |   |   |
| 3 |   | 2 |   |   |   |   |   |   |
| 4 |   |   |   | 5 |   | 4 |   | 7 |
| 5 |   |   | 8 |   |   | 3 |   |   |
| 6 |   |   | 1 |   | 9 |   |   |   |
| 7 | 3 |   |   | 4 |   | 2 |   |   |
| 8 |   | 5 |   | 1 |   |   |   |   |
| 9 |   |   |   | 8 |   | 6 |   |   |

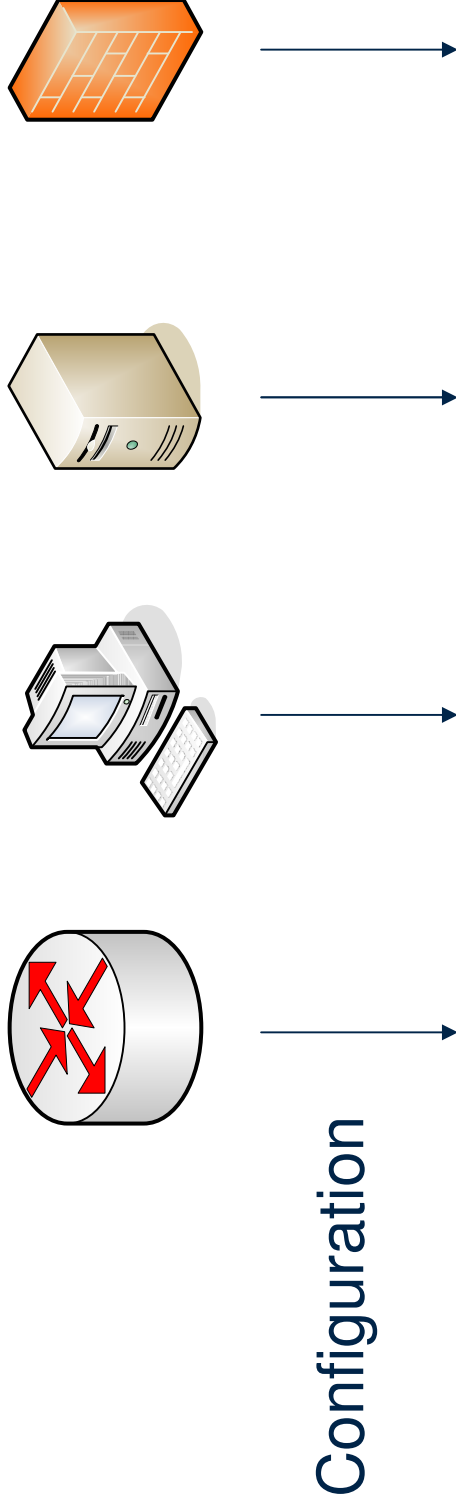
$$A(8, 8) \approx 9 \vee A(8, 8) \approx 8$$



$$A(8, 8) \approx 9 \quad A(8, 8) \approx 8$$



# LAN Analysis



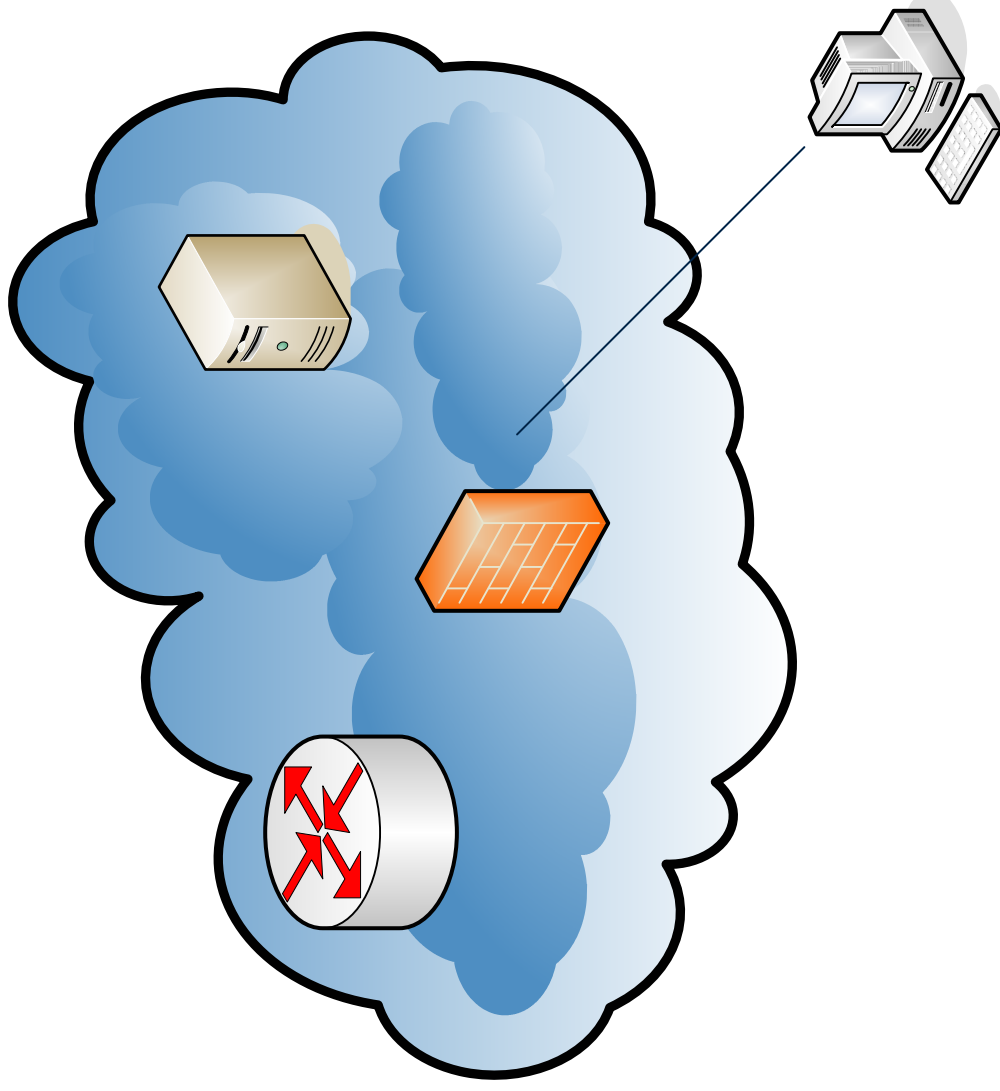
+ First-Order Model of the Components



Properties

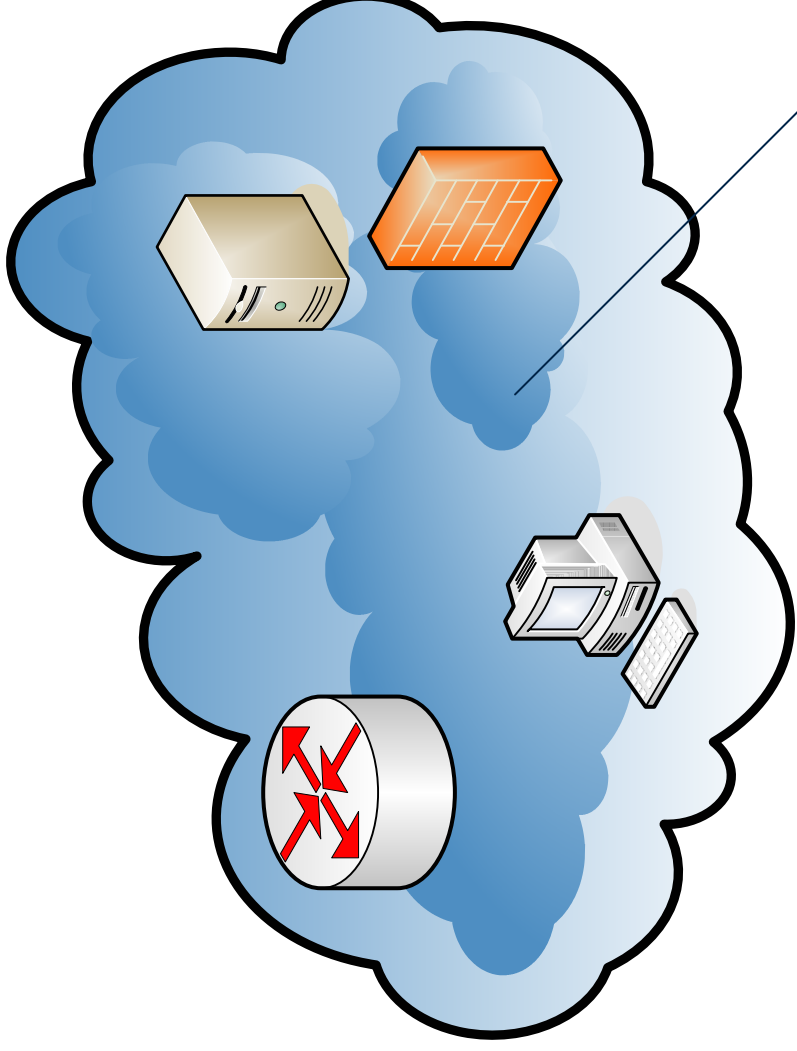


# Properties: Client



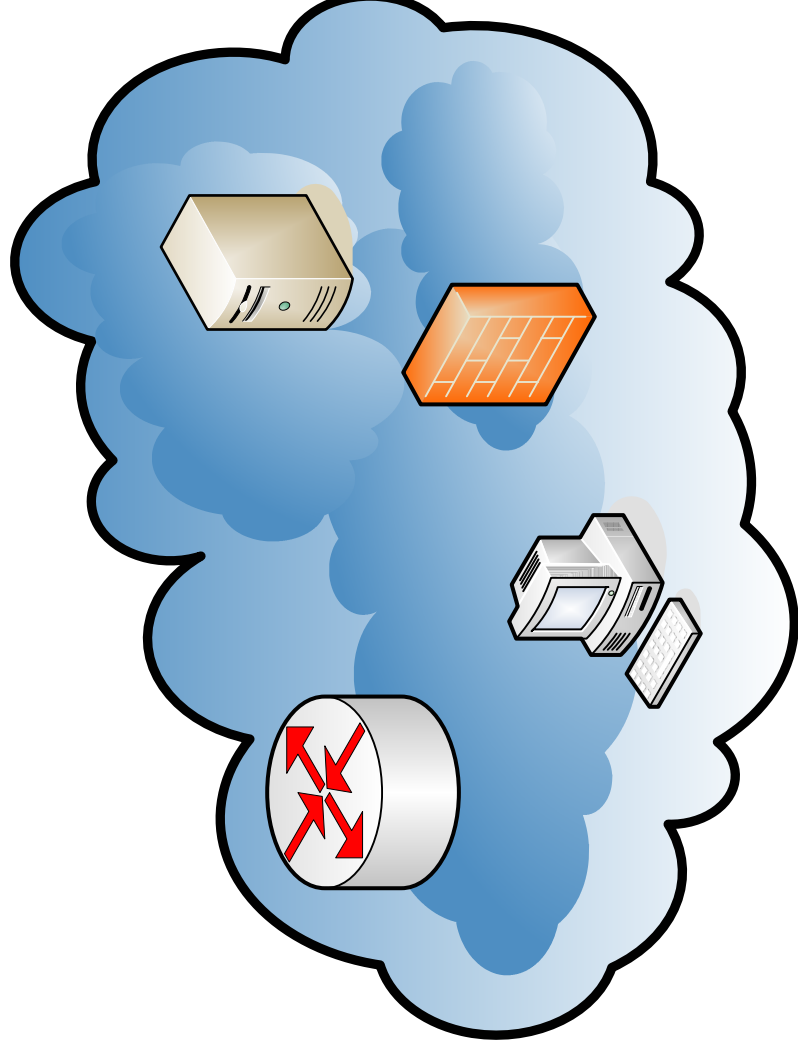


# Properties: Intruder



# Properties: Fault Analysis

max planck institut  
informatik



Uwe Waldmann, Christoph Weidenbach

Automated Reasoning SS06

# The Router



max planck institut  
informatik

```
Sent(epacket(incoming-net, router-mac, src-mac, e-ip,  
            ippacket(ip-src, ip-dst, ip-proto, ip-data)))) ^  
RouteEntry(route(router,dst-netmask,dst-net-addr,outgoing-net))  
ipand(ip-dst,dst-netmask) ≈ dst-net-addr ^
```



```
Sent(epacket(outgoing-net, dst-mac, src-mac, e-ip,  
            ippacket(ip-src, ip-dst, ip-proto, ip-data))))
```



# Example: DHCP over Firewall



# Automated Reasoning: Automation of Logic

- Syntax
- Semantics
- Calculus
- Reduction + Simplification
- Efficient Algorithms
- Proper Implementation
- Right Applications
- Right Modelling

