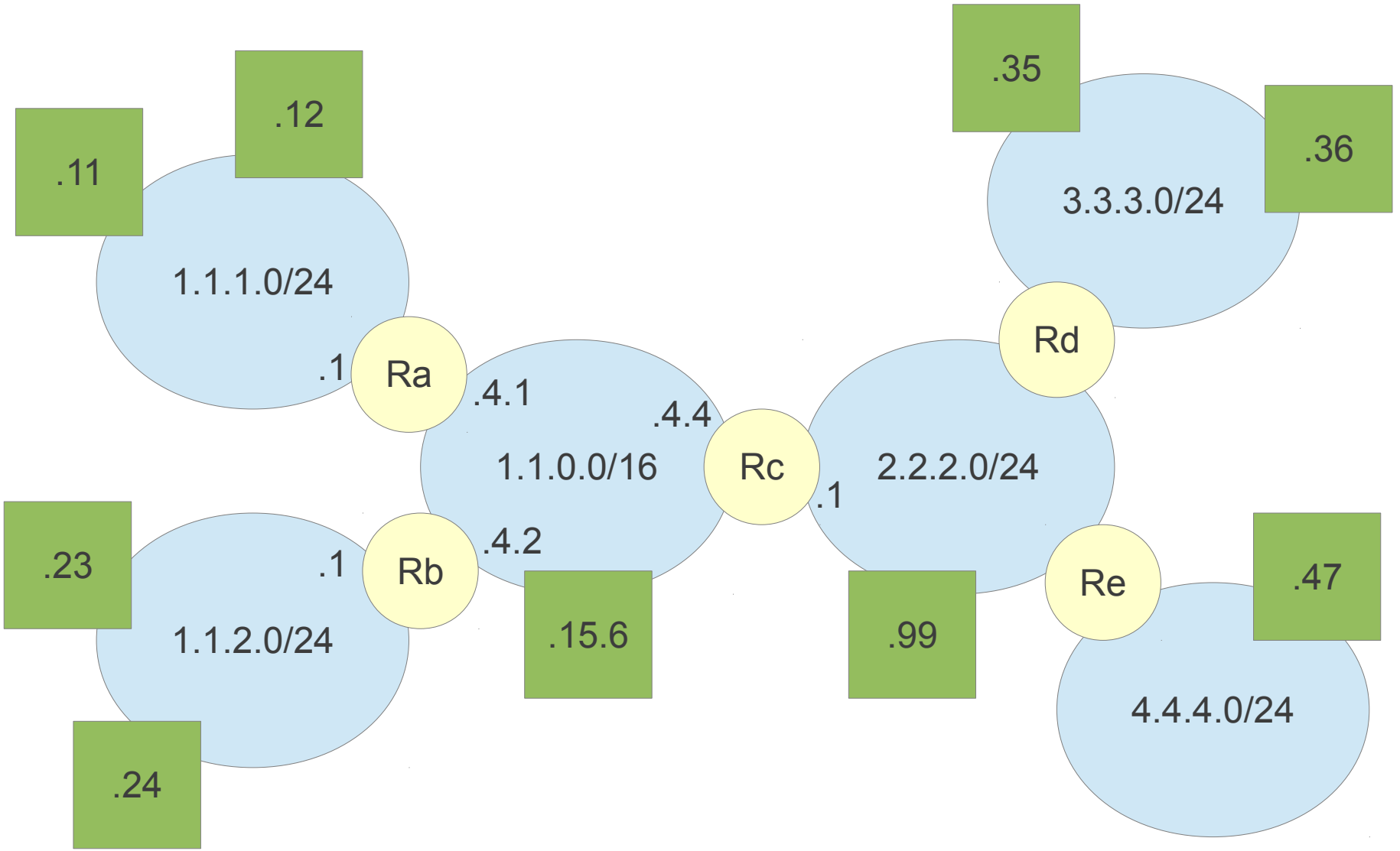
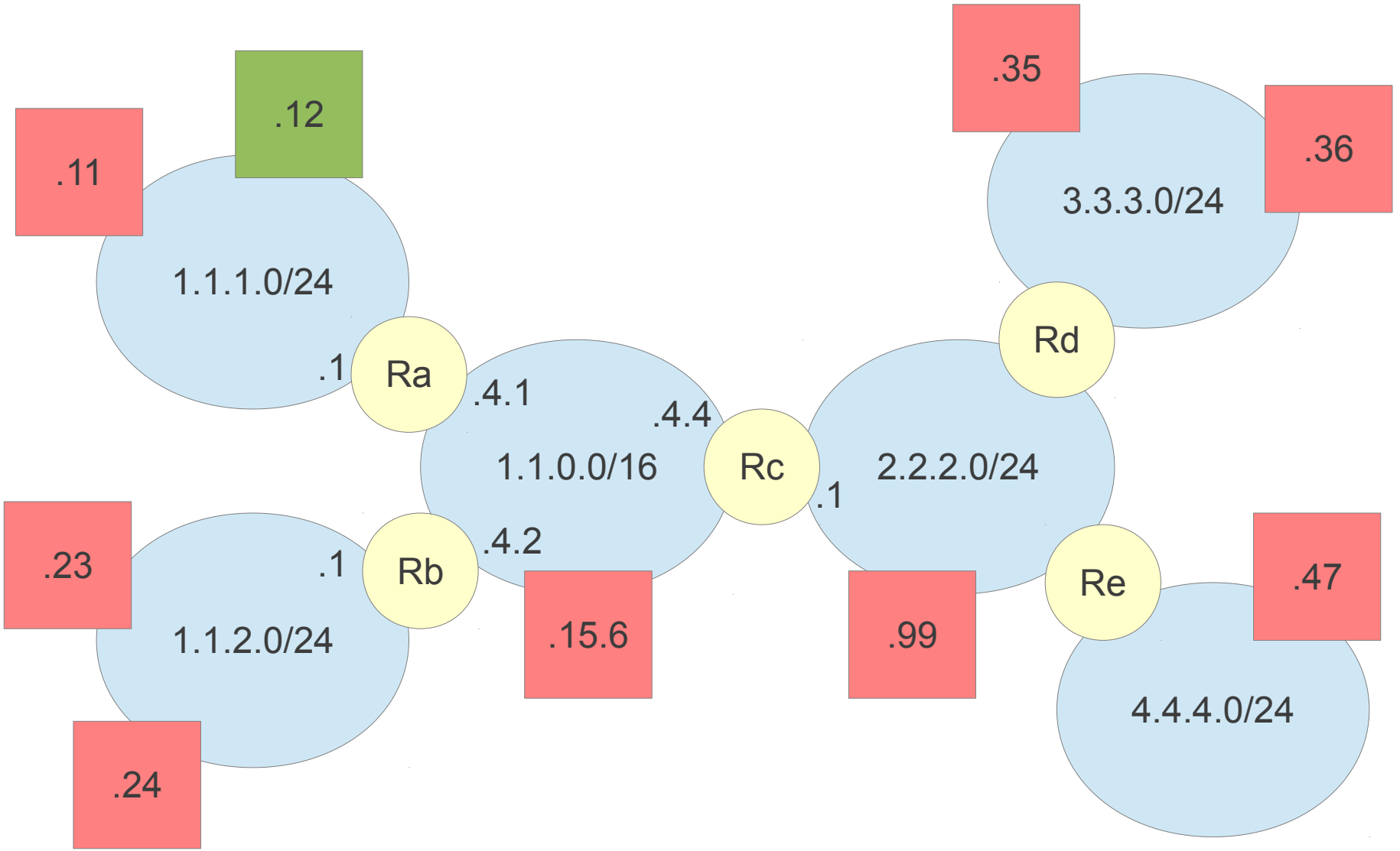
Using a firewall to control traffic in networks

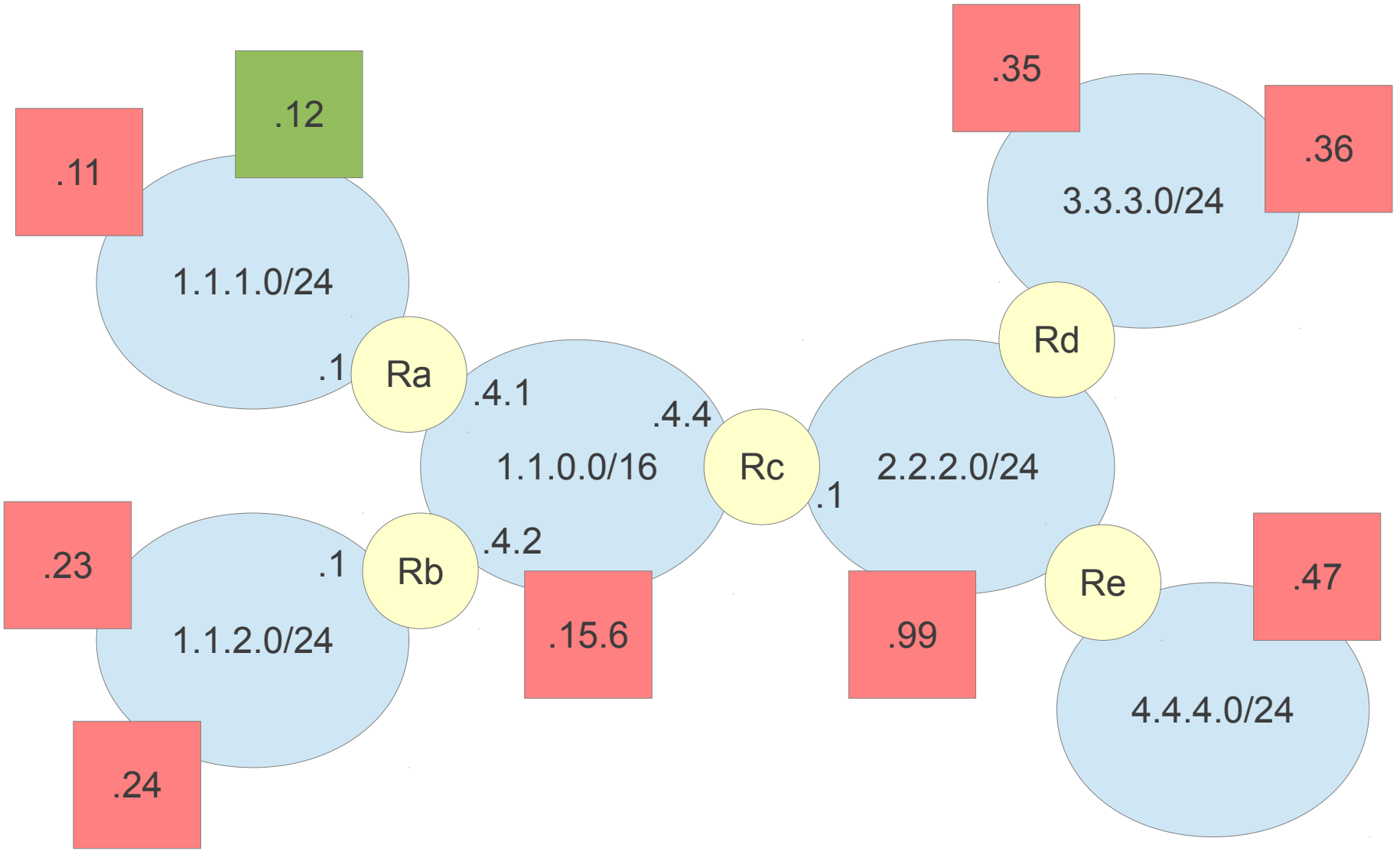
Example Network



Firewall on 1.1.1.12

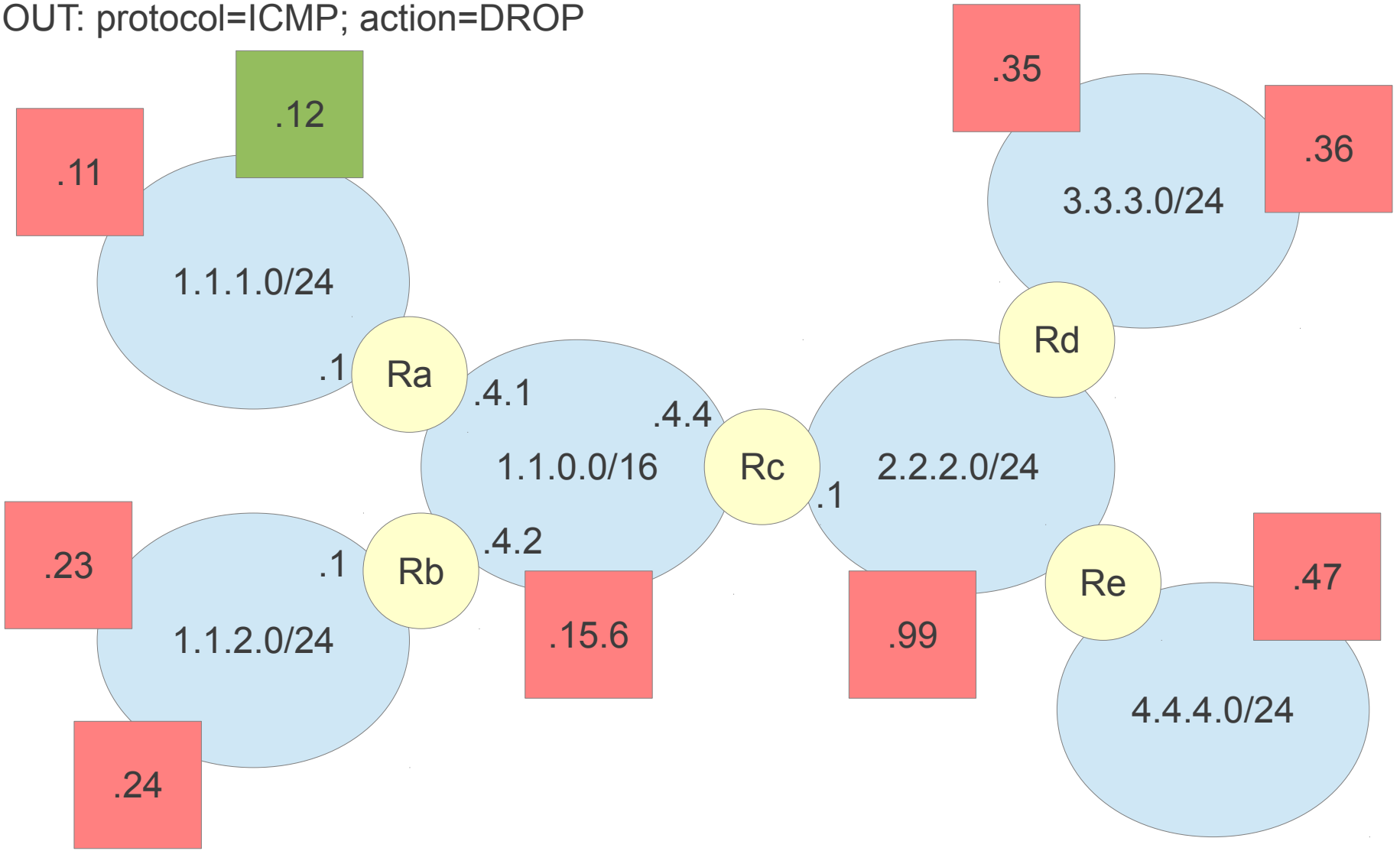


Block Ping


.12
.11
1.1.1.0/24
.1
Ra
.4.1
.4.4
1.1.0.0/16
Rc
.35
.36
3.3.3.0/24
Rd
2.2.2.0/24
.1
.23
.1
Rb
.4.2
1.1.2.0/24
.15.6
.99
Re
.47
4.4.4.0/24
.24

Block Ping

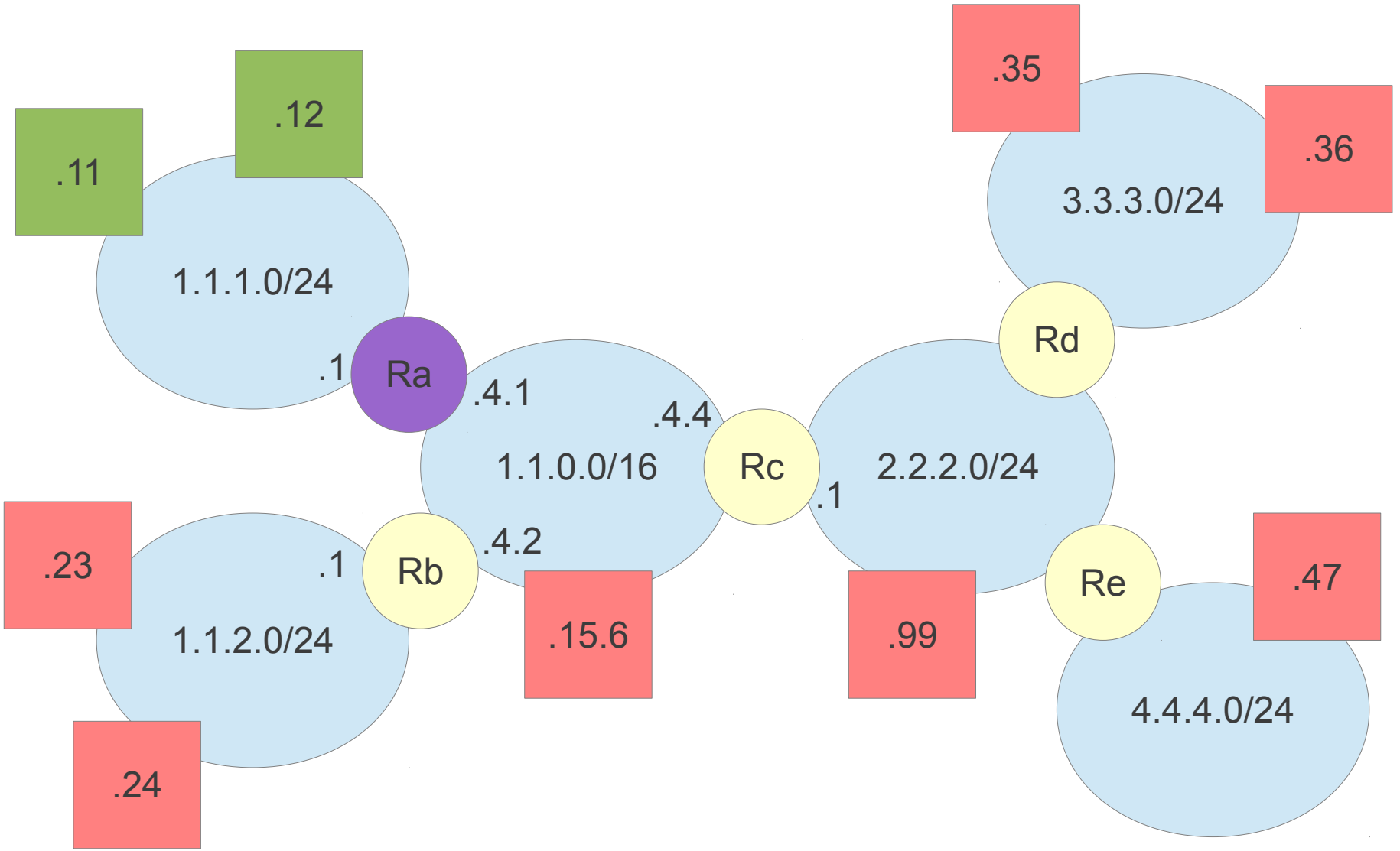
IN: protocol=ICMP; action=DROP
OUT: protocol=ICMP; action=DROP



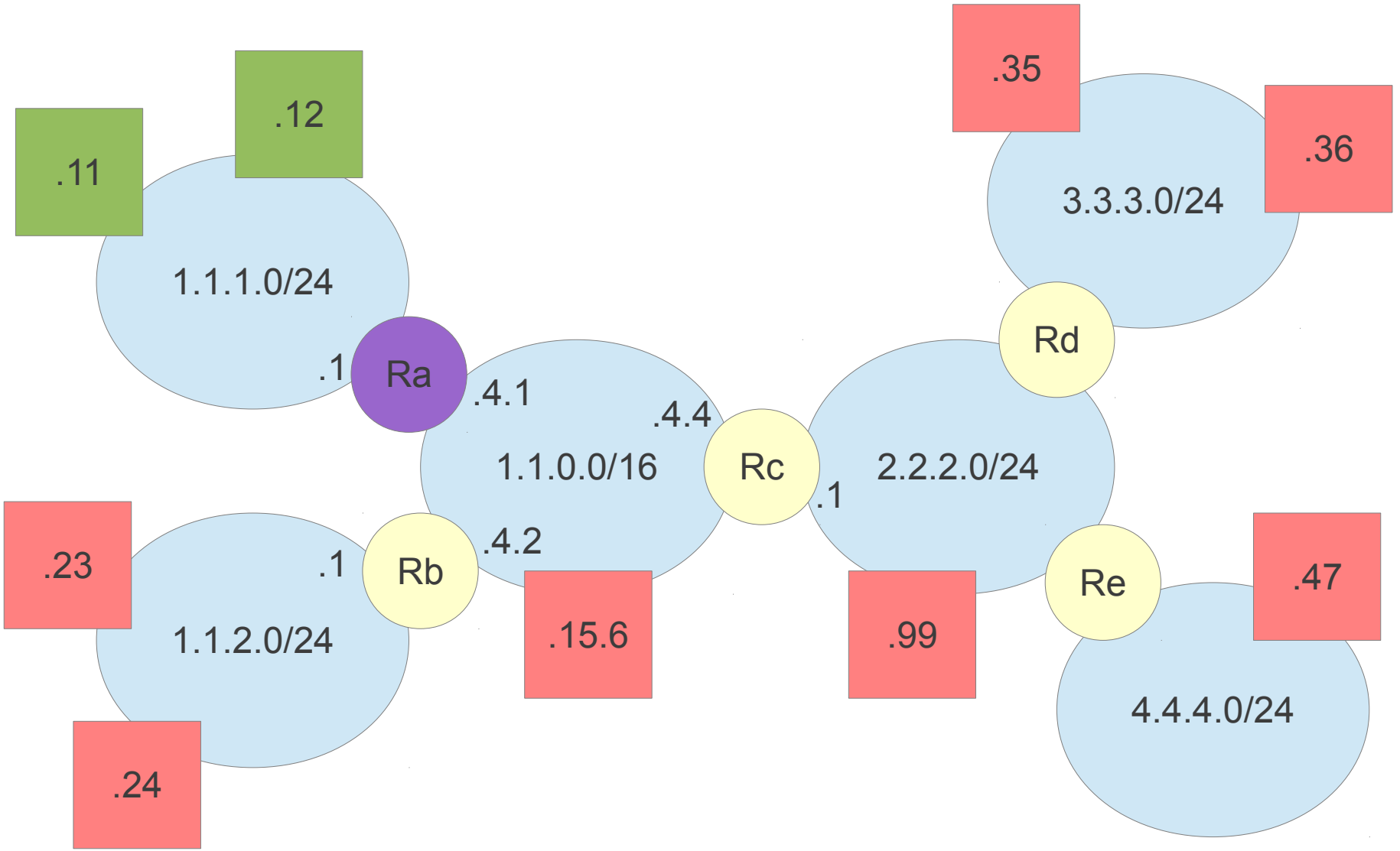
Firewall contains rules

- Each packet is checked against firewall rules
- If conditions in rule are true then perform action on that packet (eg. DROP, ACCEPT)
- If no rules match, then perform default action
- Multiple rules are combined to create a table

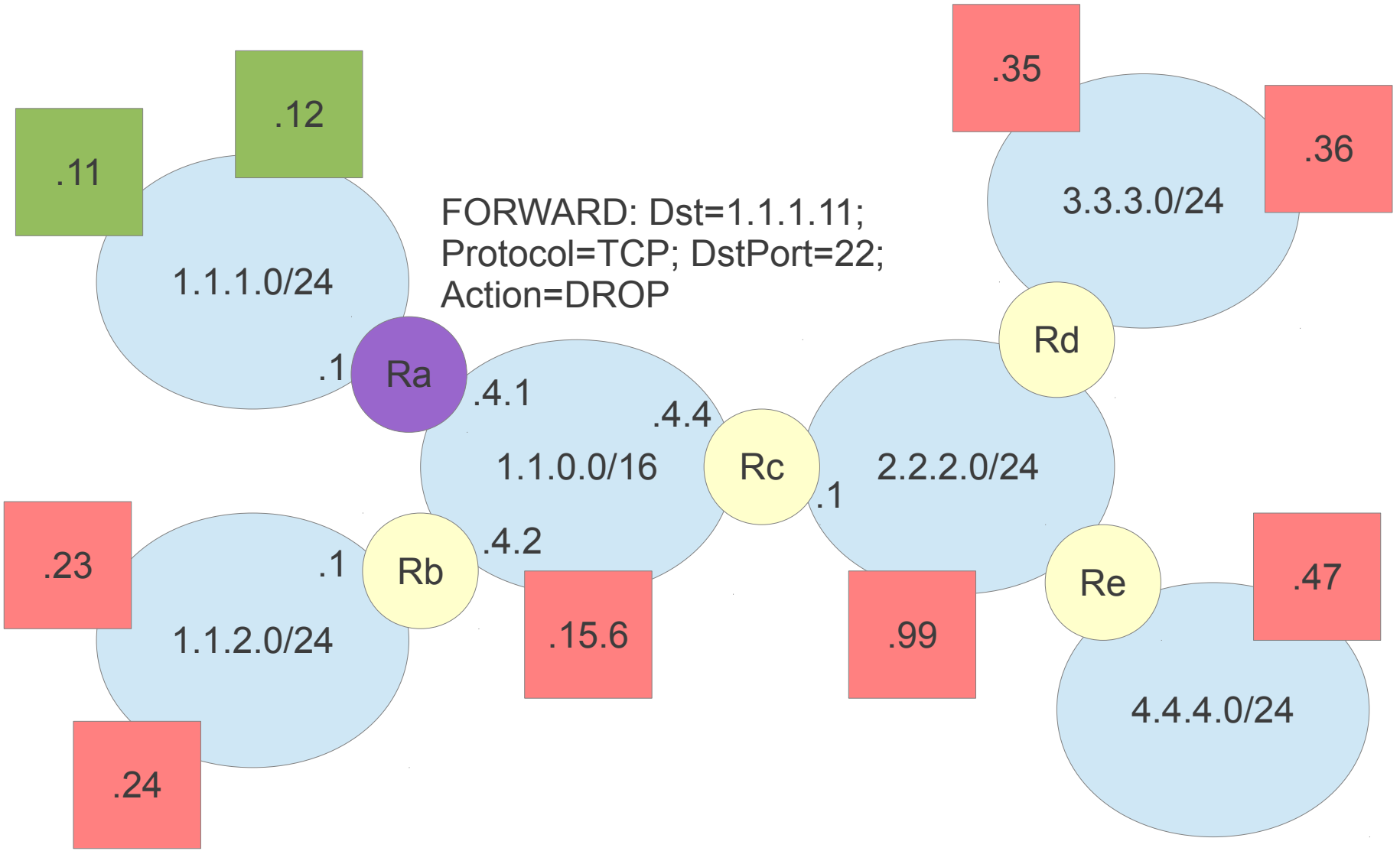
Firewall on Router Ra



Block Access to SSH Server on .11



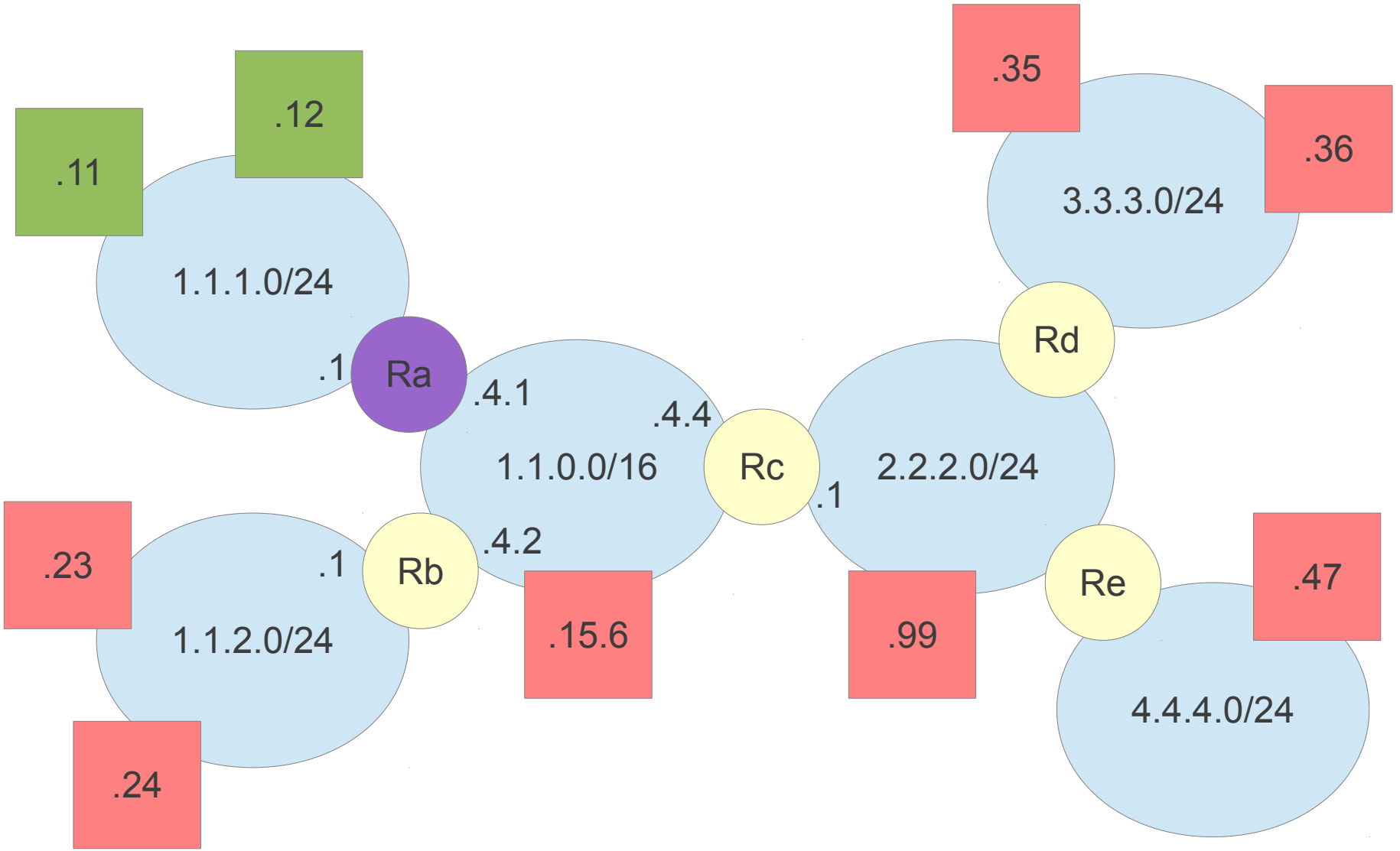
Block Access to SSH Server on .11



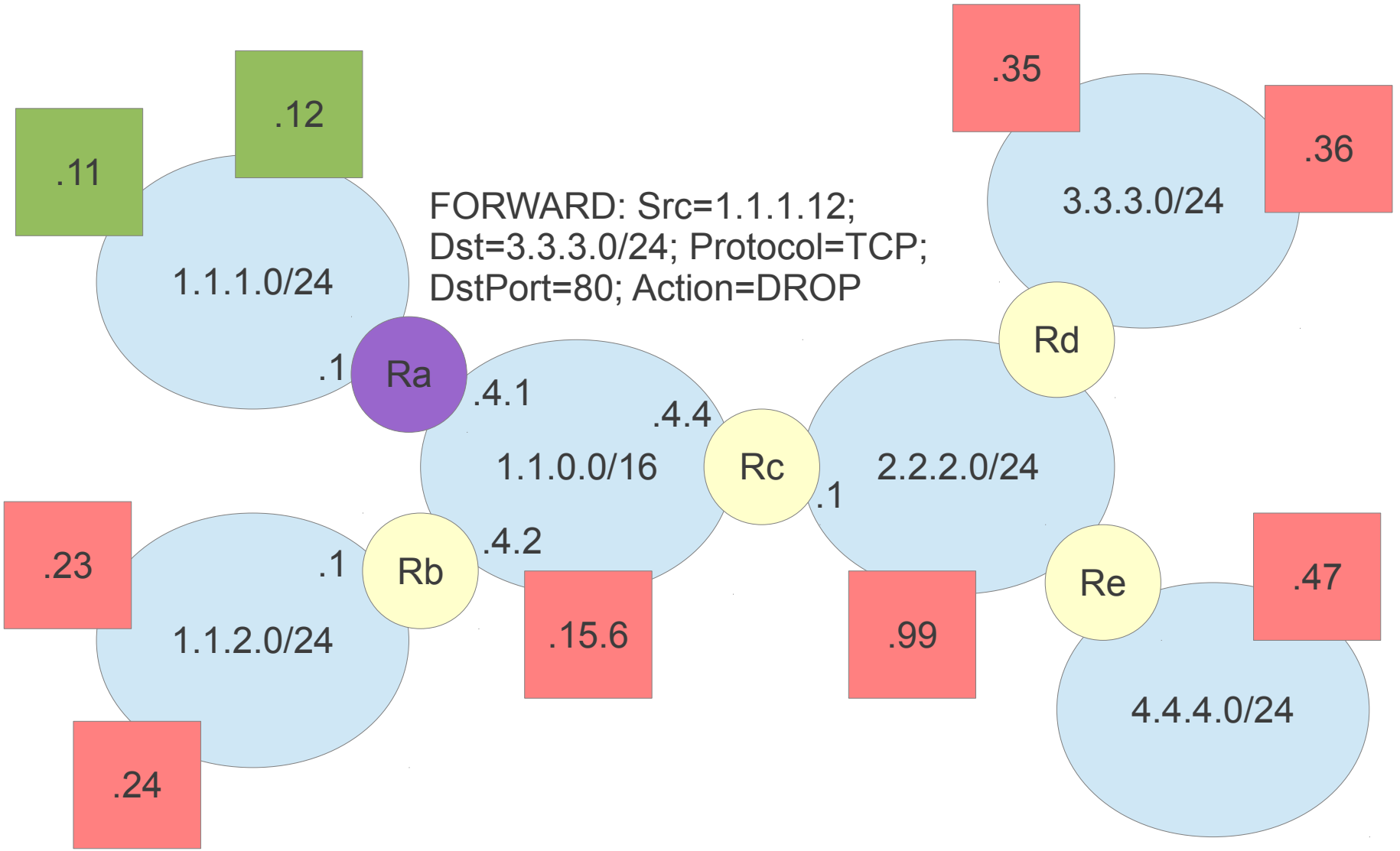
Firewall can have different rules

- INPUT: Applies only to packets destined to this computer
- OUTPUT: Applies only to packets created by this computer
- FORWARD: Applies only to packets going through this computer
- These are called *chains*

Block Access to Web Servers on Network 3.3.3.0/24 for .12



Block Access to Web Servers on Network 3.3.3.0/24 for .12



Firewall Rules Viewed as Table

Firewall table for FORWARD:

Rule	Source	Dest.	Protocol	Action
1	*	1.1.1.11:22	TCP	DROP
2	1.1.1.12:*	3.3.3.0/24:80	TCP	DROP
Default	*	*	*	ACCEPT

When packet arrives at firewall, rules are checked row-by-row. If a rule matches, the ACTION is taken and no further rules are checked.

Separate tables for INPUT, OUTPUT and FORWARD chains.