HACS 101

Week 6 - Firewall

What People Think Firewalls Do

DEPARTMENT OF DEFENSE

DES 128 BIT ENCRYPTED SECURITY

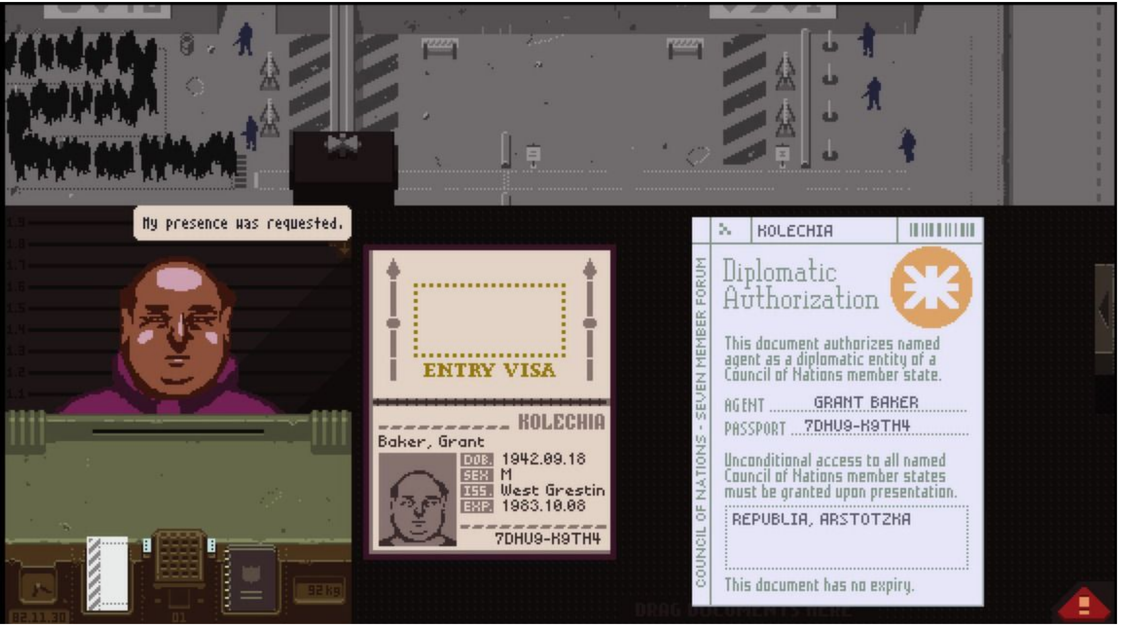
RESTRICTED ACCESS ONLY

Pedro Ruiz-Garcia

Authorized access code:

••••••••••••

What Firewalls Really Do



My presence was requested.

ENTRY VISA

KOLECHIA

Baker, Grant

DOB 1942.09.18
SEX M
ISS. West Grestin
EXP. 1983.10.08

7DHU9-K9TH4

KOLECHIA

Diplomatic Authorization

This document authorizes named agent as a diplomatic entity of a Council of Nations member state.

AGENT GRANT BAKER
PASSPORT 7DHU9-K9TH4

Unconditional access to all named Council of Nations member states must be granted upon presentation.

REPUBLIA, ARSTOTZKA

This document has no expiry.

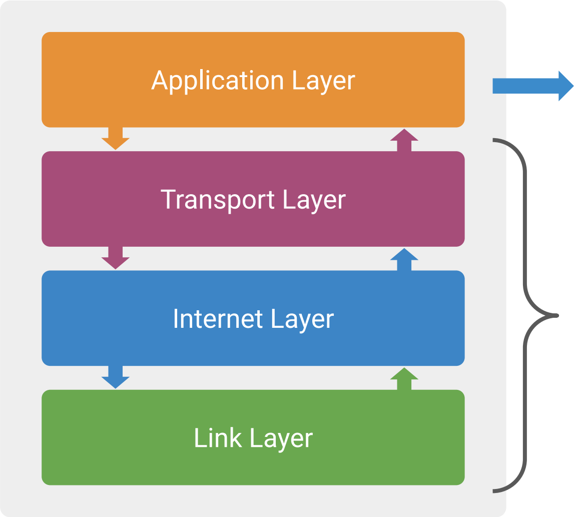
COUNCIL OF NATIONS - SEVEN MEMBER FORUM

What is a Firewall?

A system that

- monitors incoming and outgoing network traffic
- permits or blocks data packets based on predefined rules

Firewalls vs Intrusion Detection/Prevention Systems



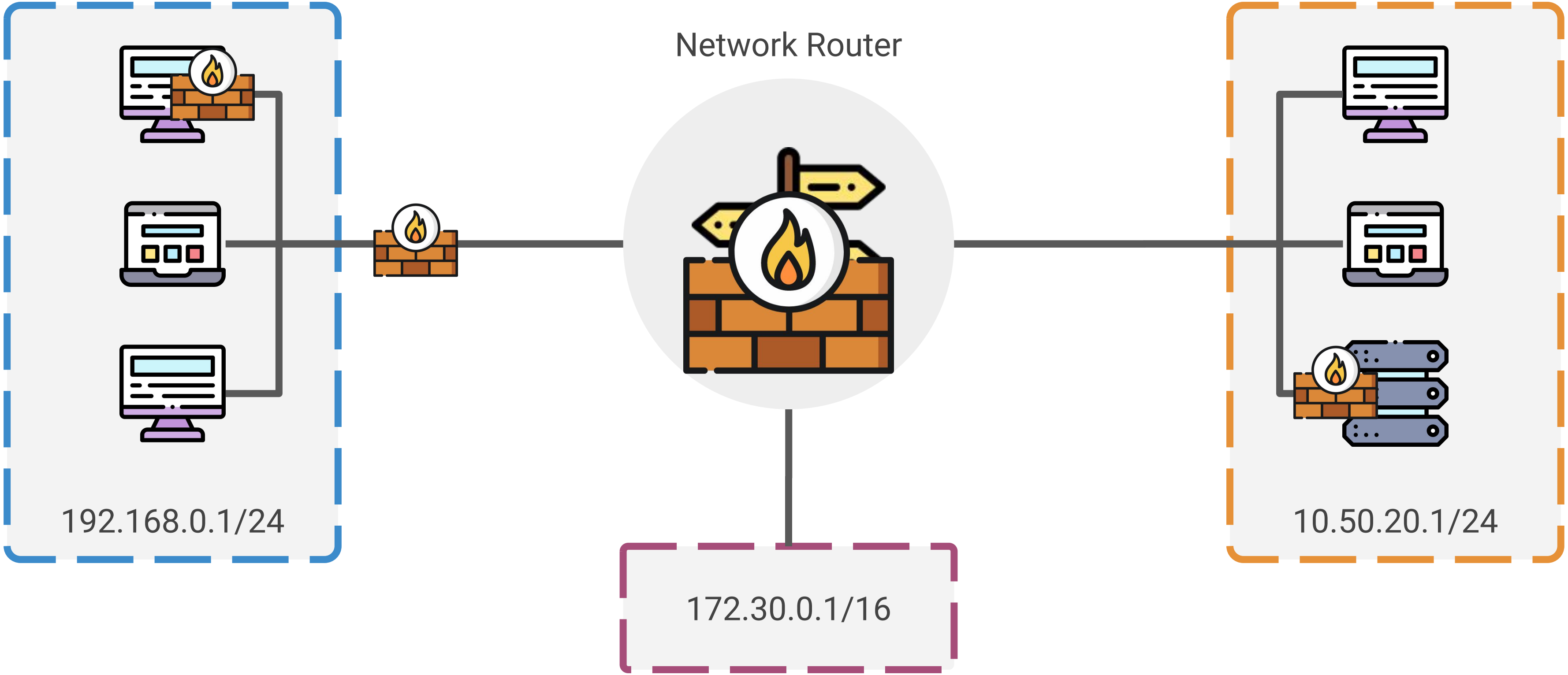
Typical firewalls will not inspect this layer

Typical firewalls operate on IP addresses and port numbers

They inspect a packet for IP & port and make a decision to allow or disallow based on the predefined rules

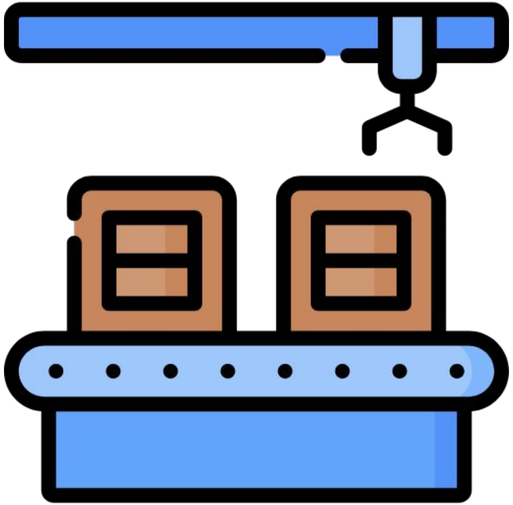
Intrusion Detection Systems (IDS) and **Intrusion Prevention Systems** (IPS) can additionally operate on the application layer and conditionally evaluate packet data (but requires more processing power)

Where can Firewalls Live?



Typical Firewall Filtering Criteria

- Network Interface
- Network protocol (IP, TCP, UDP, etc)
- Traffic direction (inbound or outbound)
- Source or destination IP address
- Source or destination port number (TCP & UDP)
- Connection State (TCP)
- Data transfer rate



Each packet is individually inspected to see if any of the filtering criteria match any rules

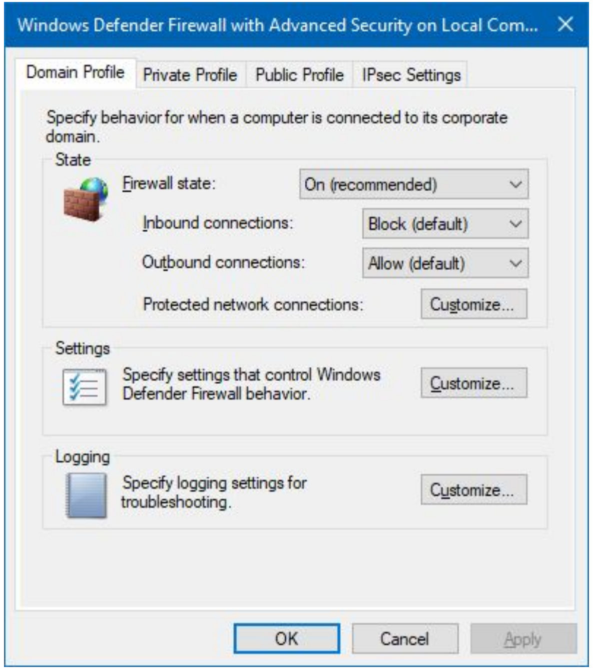
The Processing of a Packet

if packet matches a rule

- if ACCEPT, send packet to its destination
- if REJECT, stop the packet and inform sender via ICMP
- if DROP, stop the packet silently

else use default policy (ACCEPT, REJECT, DROP)

Firewalls



Windows Defender Firewall with Advanced Security on Local Com... ✕

Domain Profile | Private Profile | Public Profile | IPsec Settings

Specify behavior for when a computer is connected to its corporate domain.

State

Firewall state: On (recommended)

Inbound connections: Block (default)

Outbound connections: Allow (default)

Protected network connections: Customize...

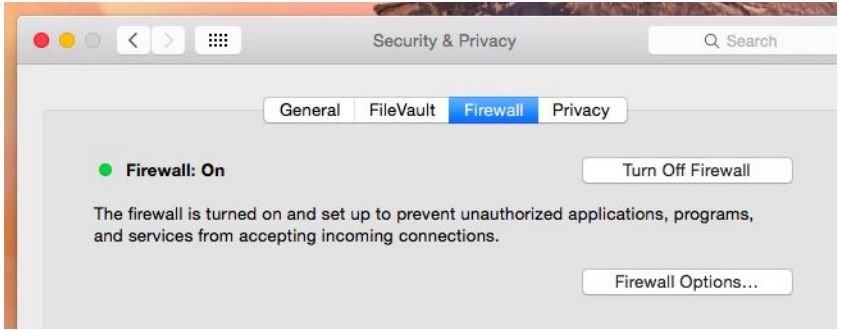
Settings

Specify settings that control Windows Defender Firewall behavior. Customize...

Logging

Specify logging settings for troubleshooting. Customize...

OK | Cancel | Apply



Security & Privacy

Search

General | FileVault | Firewall | Privacy

● **Firewall: On** | Turn Off Firewall

The firewall is turned on and set up to prevent unauthorized applications, programs, and services from accepting incoming connections.

Firewall Options...

CLI > GUI

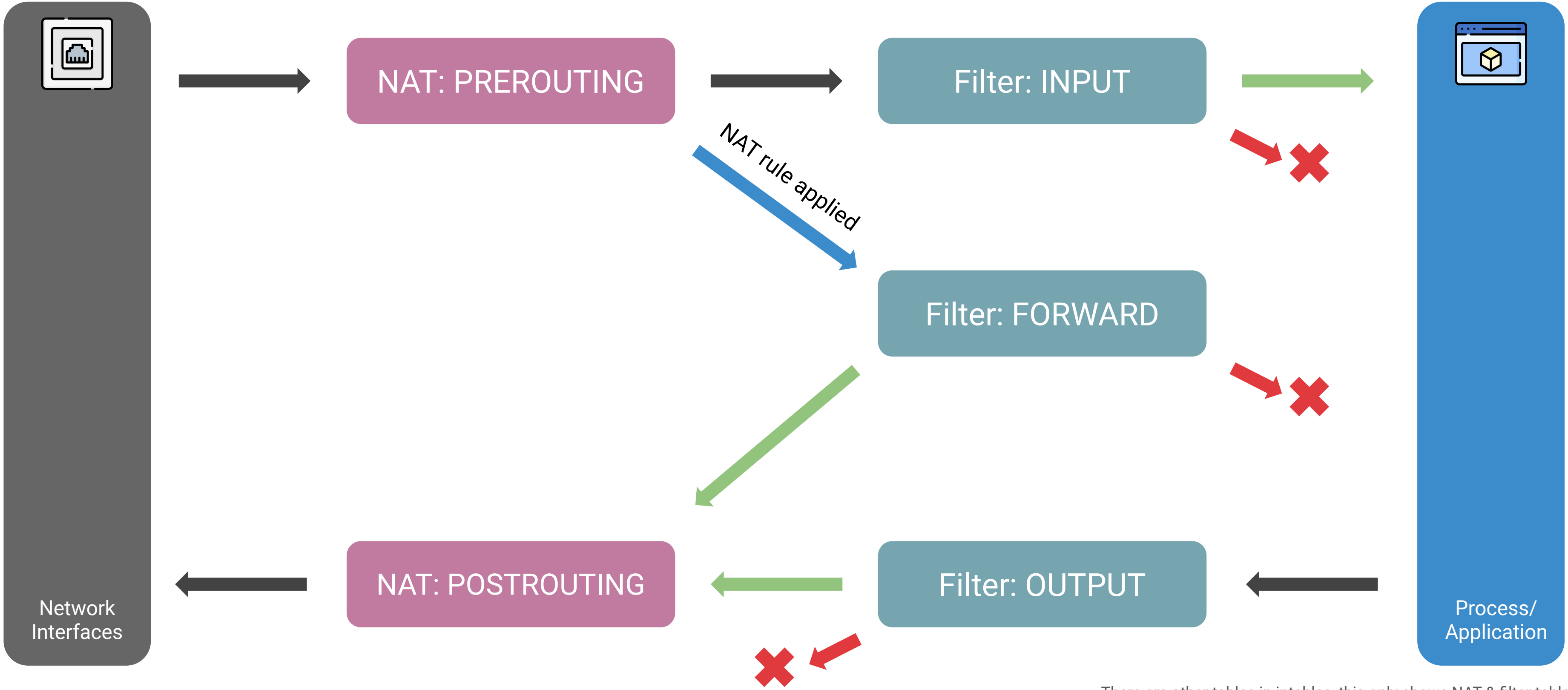
`iptables`

Didn’t we use `iptables` for NAT tables?

Yes, `iptables` control both the “NAT table” and the “filter table” - used to allow or disallow packets

(“filter table” is the default table, so you don’t have to specify the table in your `iptables` command)

`iptables` Chains - NAT & Filter Tables



There are other tables in iptables, this only shows NAT & filter tables

How are `iptables` Rules Evaluated?

#	Rule	Policy
1	Source IP: 128.8.1.123	DROP
2	Source Network: 128.8.0.0/16	ACCEPT
3	Any	DROP

Rules are evaluated based on precedence, from "top to bottom"

If a rule matches, the remaining rules are not evaluated

📦 Source: 128.8.1.123

📦 Source: 128.8.1.2

📦 Source: 8.8.8.8

Using the `iptables` Command to Filter

```
iptables
  --insert <chain name>
  --source <ip or CIDR network>
  --destination <ip or CIDR network>
  --protocol <tcp, udp, etc>
  --source-port <port number>
  --destination-port <port number>
  --jump <ACCEPT, REJECT, DROP>
```

```
iptables --insert OUTPUT --source 10.3.0.2 --destination 10.3.0.1 --protocol
tcp --source-port 22 --destination-port 5000 --jump DROP
```

Drop all outbound TCP traffic from 10.3.0.2:22 to 10.3.0.1:5000

Insert vs Append

`iptables --insert`

Prepends the rule
i.e. add the rule as rule #1 and shift every other rule by one

`iptables --append`

Appends the rule
i.e. add the rule as rule #n+1 and all other rules remain the same

Persisting Firewall Rules

Iptables rules get reset on reboot

(which is great if you messed up and need a reset)

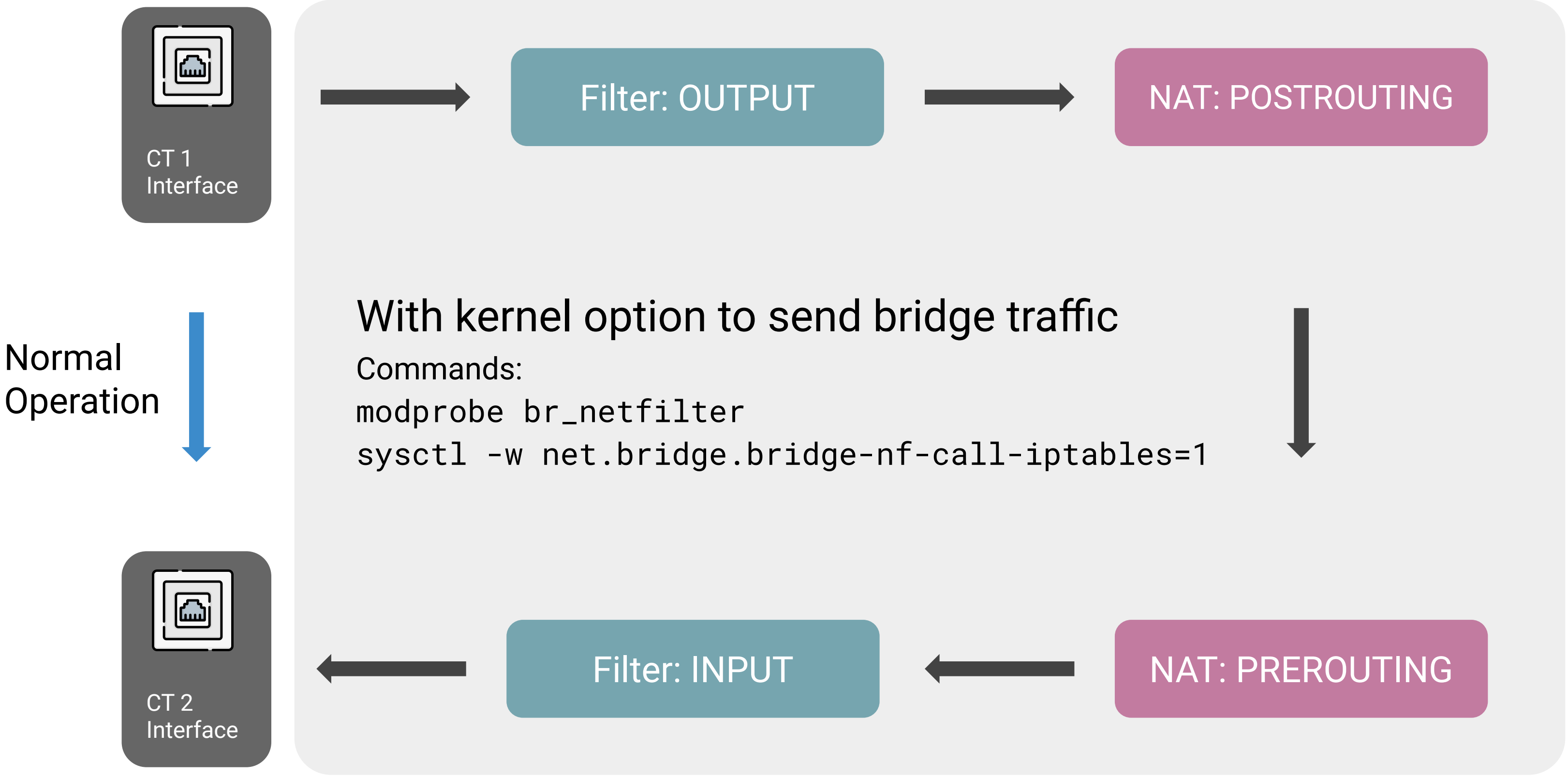
`iptables-save`

Outputs a file with a listing of your iptables rules

`iptables-restore`

Restores your iptables rules using the output listing from `iptables-save`

Packets Between Containers (Linux Bridges)

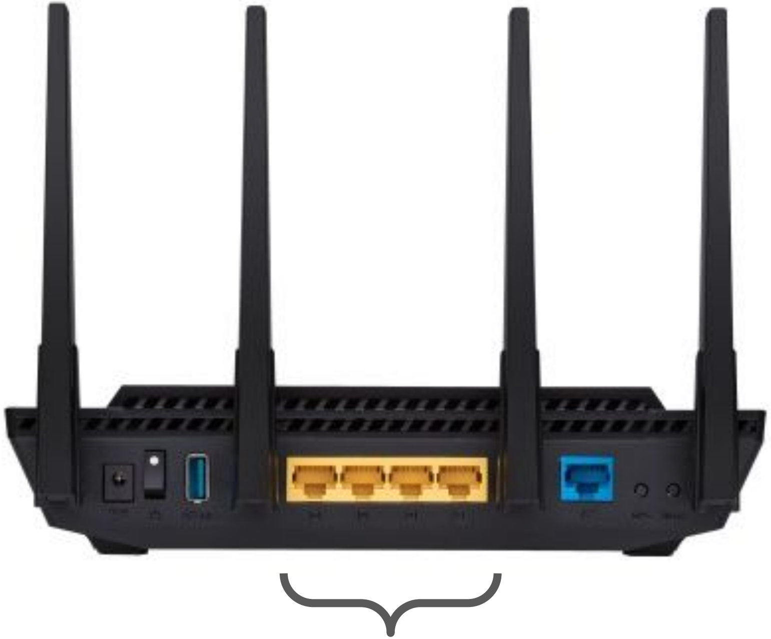


With kernel option to send bridge traffic

Commands:

```
modprobe br_netfilter
sysctl -w net.bridge.bridge-nf-call-iptables=1
```

Visualizing Linux Bridges



These LAN ports act like bridges, data gets forwarded between each other without any *routing*

Reminders

Quiz 6

Due Friday **6:00pm**

Homework 6

Due Sunday 11:59pm