CS183

Instructor: Ali Davanian
(Slides were adopted from Brian Crites and Alireza Abdoli)

L3 Advanced Topics

Routing and Security

Logistics

- Please start working on your project ASAP (if you already haven’t)
    - Next week we’ll have a Holiday, and the week after is your last chance to get help
- Expect a Pop-up quiz quiz after the holiday
- Week 10 is only for your project presentations
    - 4 minutes per group; you’d need to sign up if you want to present
    - Not In-Person, only virtual

The Routing Table

- The routing table performs a similar function to the switching table in L2 and is responsible for making sure traffic gets to where it needs to go
- The routing table is primarily made up of the following fields:
  - Network ID & Mask represents an available network a device can route traffic to (0.0.0.0 used to route traffic not otherwise in the table)
  - Gateway (Next Hop) is the next L3 appliance interface’s IP address that must be traversed to reach the destination
  - Interface is the port* used to reach the next hop
  - Metric is the cost of getting to the next hop through the interface

IP Address ranges

Table 13.3 Historical Internet address classes

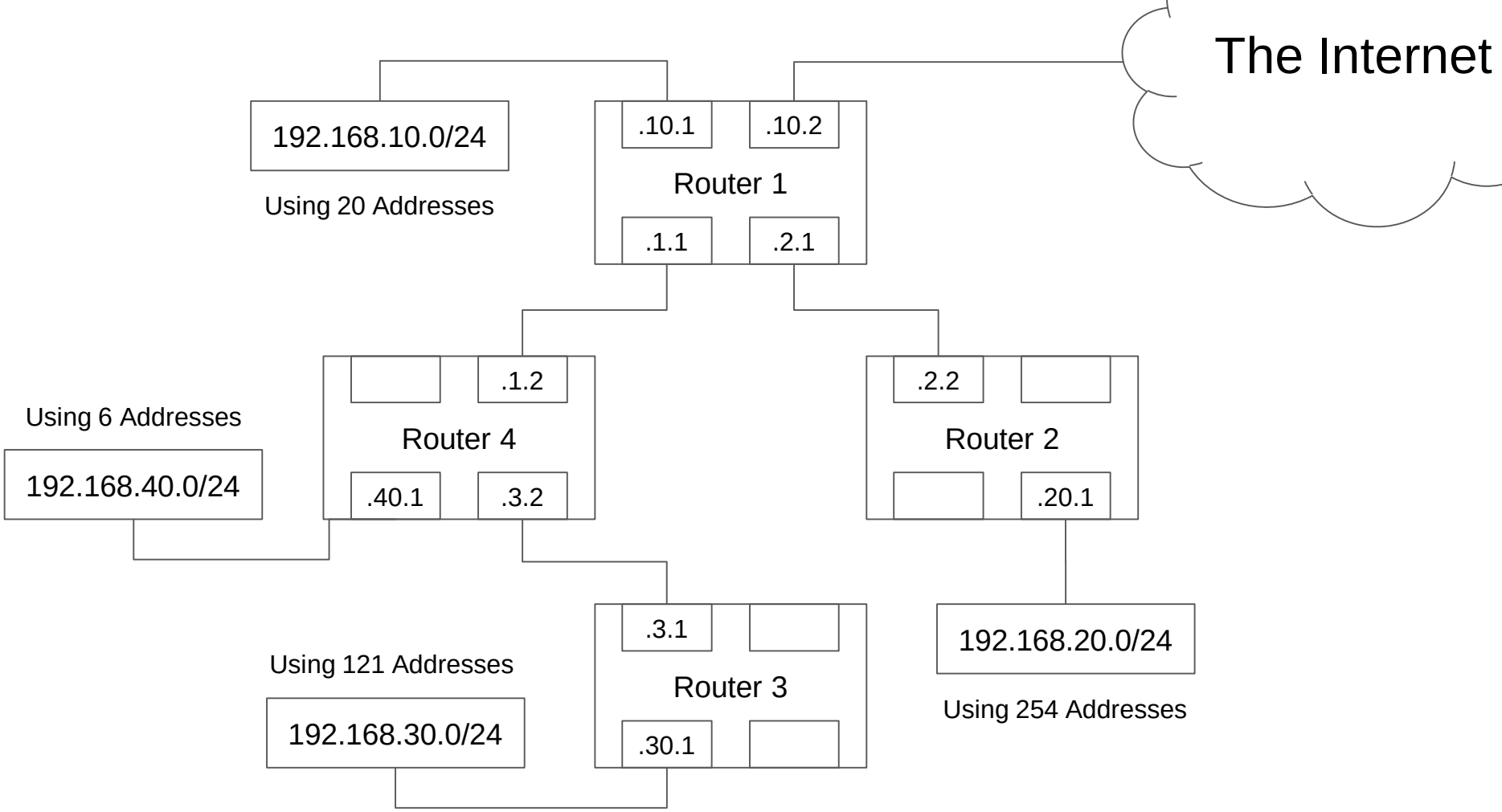
Class	1st byte[a]	Format	Comments
A	1-126	N.H.H.H	Very early networks, or reserved for DOD
B	128-191	N.N.H.H	Large sites, usually subnetted, were hard to get
C	192-223	N.N.N.H	Easy to get, often obtained in sets
D	224-239	–	Multicast addresses, not permanently assigned
E	240-254	–	Experimental addresses

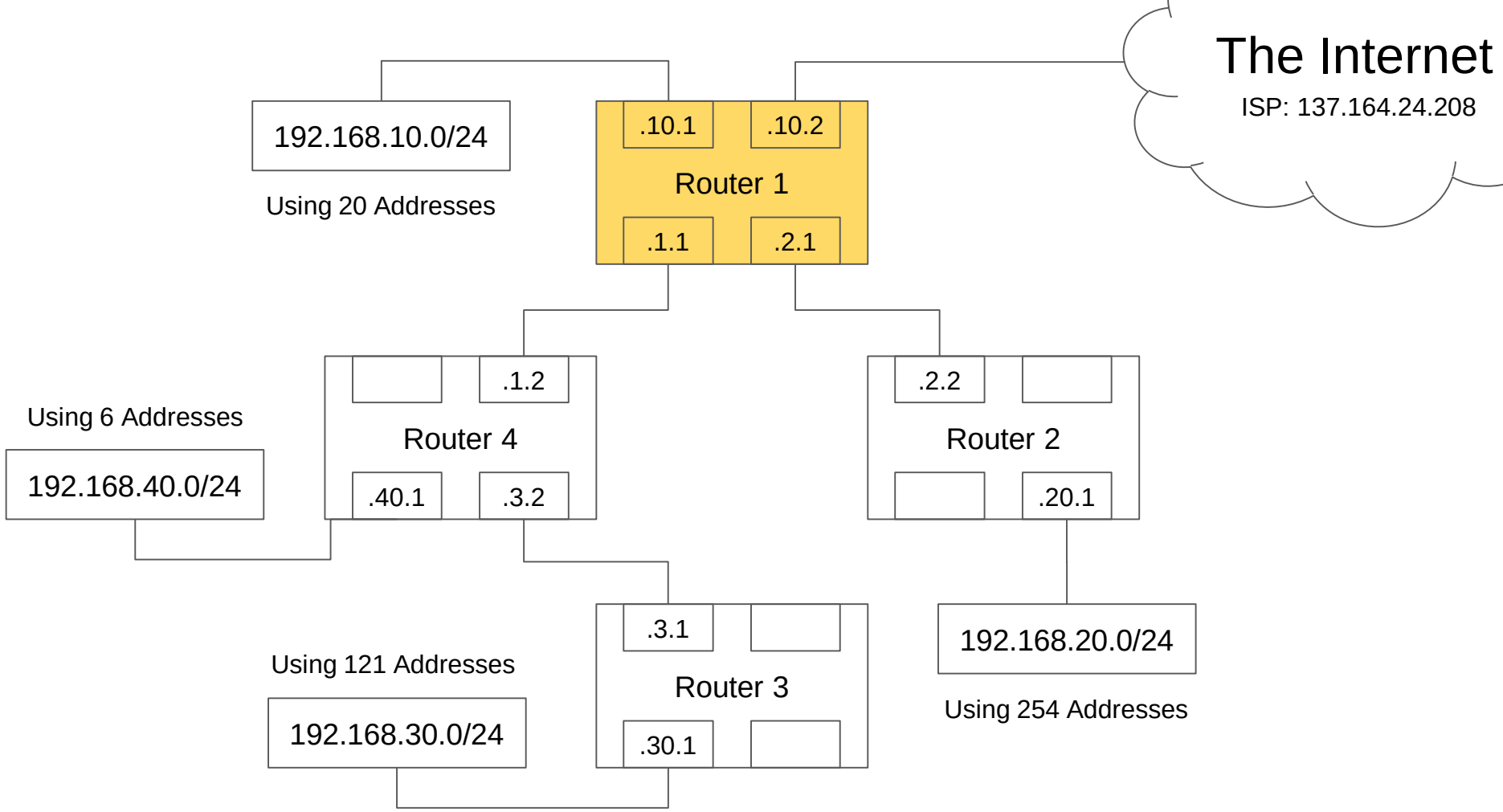
Table 13.7 IP addresses reserved for private use

IP class	From	To	CIDR range
Class A	10.0.0.0	10.255.255.255	10.0.0.0/8
Class B	172.16.0.0	172.31.255.255	172.16.0.0/12
Class C	192.168.0.0	192.168.255.255	192.168.0.0/16

Routing configuration

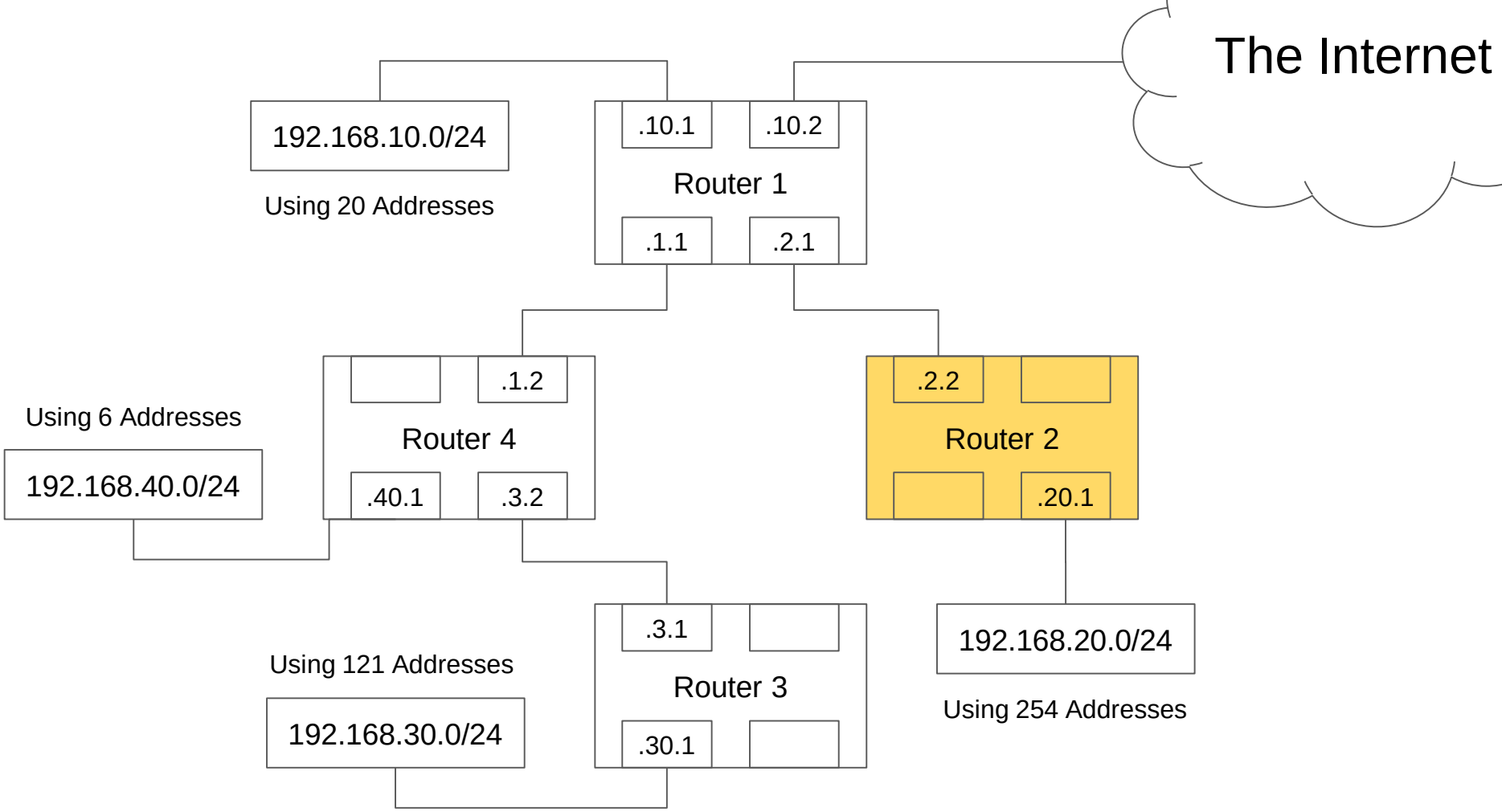
- Routing configuration can be done statically or dynamically
- In static routing, the entries are manually added to the router:
    - ip route add [subnet-CIDR] via [destination-ip] dev [local-interface]
- In dynamic routing, a routing protocol is used
    - They learn the routes automatically
    - They update the routes automatically if there is any change


The Internet
192.168.10.0/24
Using 20 Addresses
.10.1
.10.2
Router 1
.1.1
.2.1
.1.2
Router 4
.2.2
Router 2
Using 6 Addresses
192.168.40.0/24
.40.1
.3.2
.20.1
.3.1
Router 3
Using 121 Addresses
192.168.30.0/24
.30.1
192.168.20.0/24
Using 254 Addresses


The Internet
ISP: 137.164.24.208
192.168.10.0/24
Using 20 Addresses
.10.1
.10.2
Router 1
.1.1
.2.1
.1.2
Router 4
.40.1
.3.2
Using 6 Addresses
192.168.40.0/24
.2.2
Router 2
.20.1
192.168.20.0/24
Using 254 Addresses
.3.1
Router 3
.30.1
Using 121 Addresses
192.168.30.0/24

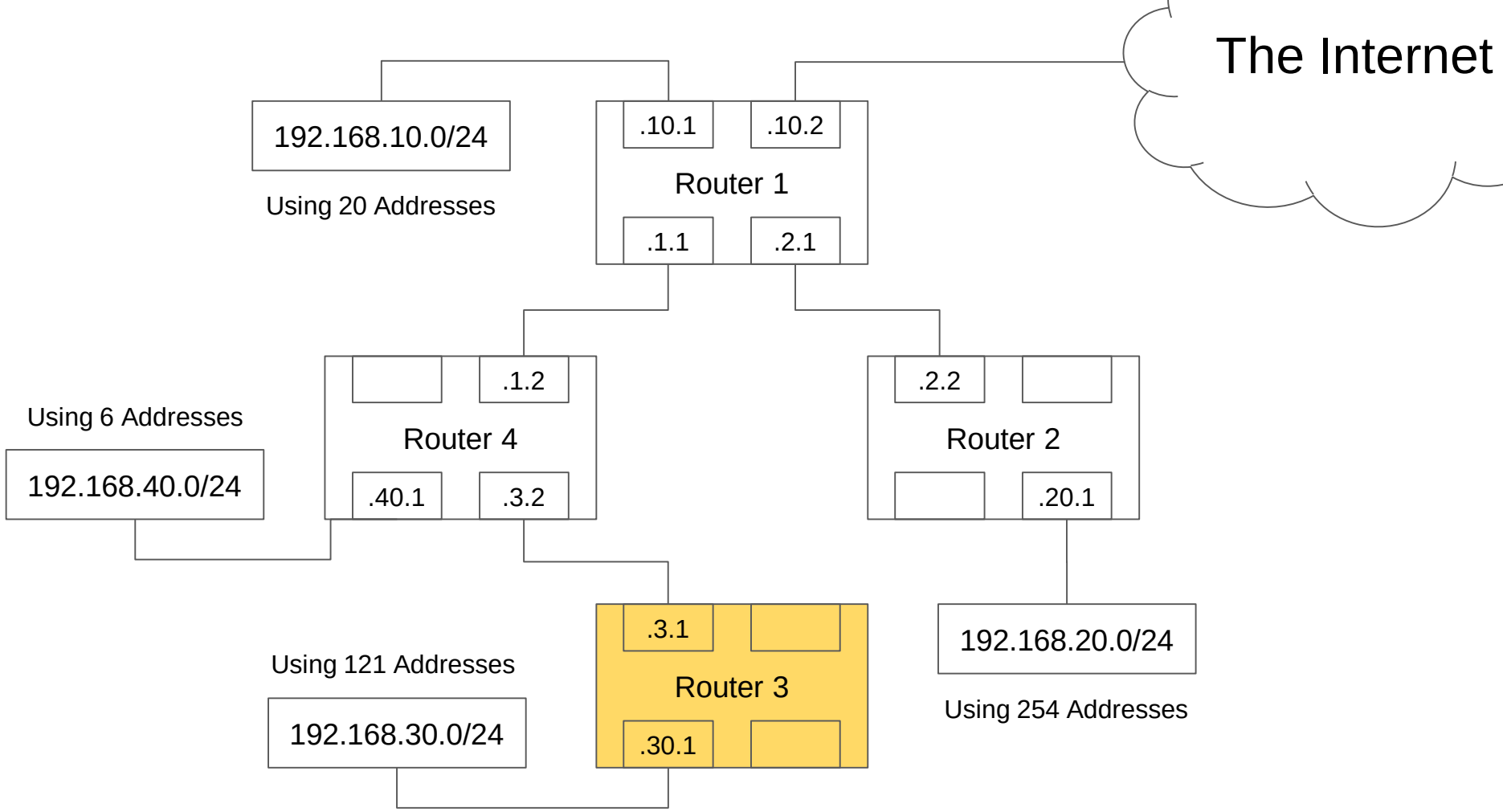
Routing Table - Router 1

Network ID	Gateway	Interface	Metric
0.0.0.0/0	137.164.24.208	192.168.10.2/24	10
192.168.10.0/24	192.168.10.1/24	192.168.10.1/24	10
192.168.20.0/24	192.168.2.2	192.168.2.1/24	10
192.168.40.0/24	192.168.1.2	192.168.1.1/24	10
192.168.30.0/24	192.168.1.2	192.168.1.1/24	10


The Internet
192.168.10.0/24
Using 20 Addresses
.10.1
.10.2
Router 1
.1.1
.2.1
.1.2
Router 4
.40.1
.3.2
Using 6 Addresses
192.168.40.0/24
.2.2
Router 2
.20.1
192.168.20.0/24
Using 254 Addresses
.3.1
Router 3
.30.1
Using 121 Addresses
192.168.30.0/24

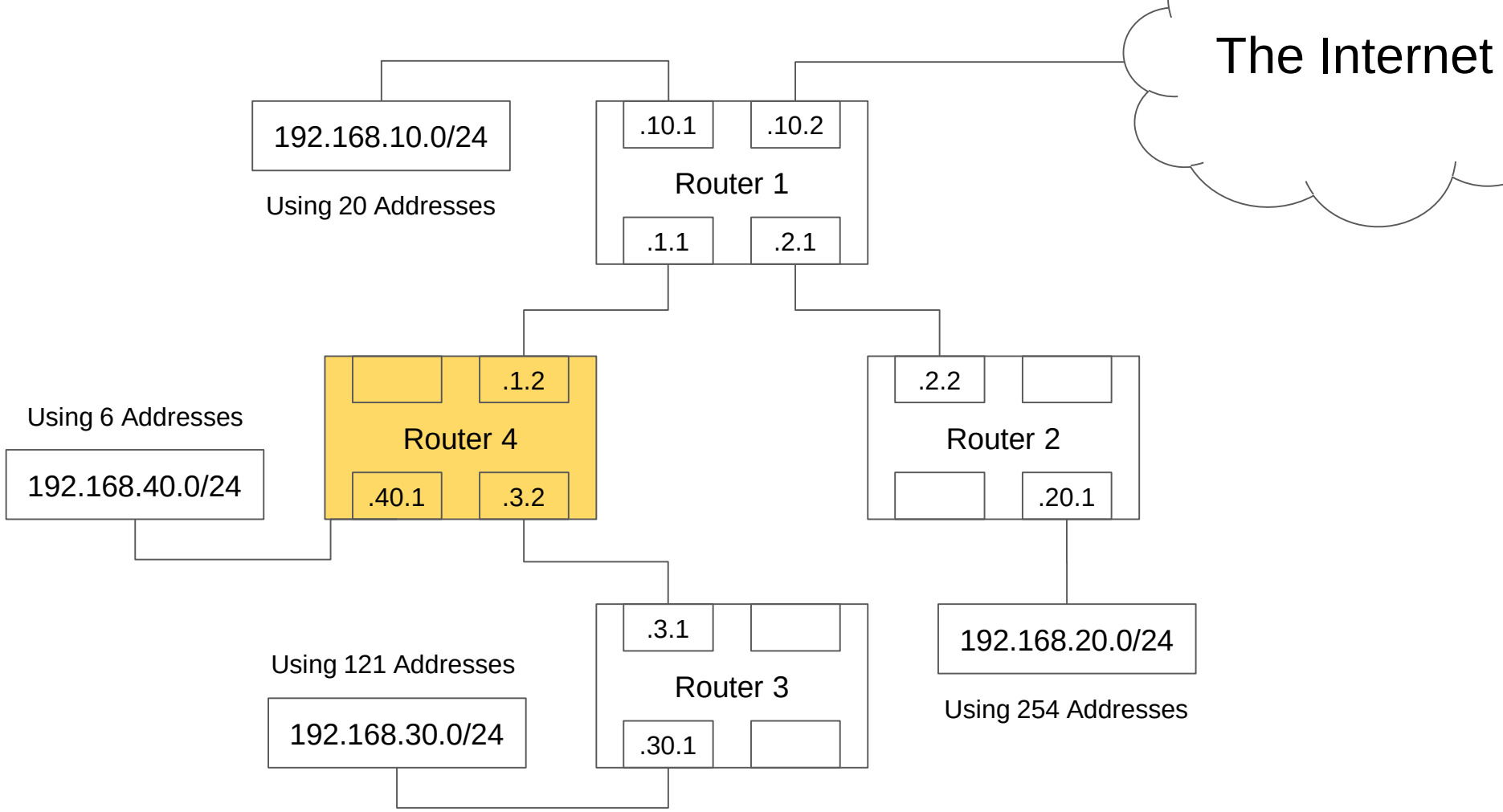
Routing Table - Router 2

Network ID	Gateway	Interface	Metric
0.0.0.0/0	192.168.2.1	192.168.2.2/24	10
192.168.20.0/24	192.168.20.1/24	192.168.20.1/24	10
~~192.168.30.0/24~~	~~192.168.2.1~~	~~192.168.2.2/24~~	~~10~~
~~192.168.40.0/24~~	~~192.168.2.1~~	~~192.168.2.2/24~~	~~10~~
~~192.168.10.0/24~~	~~192.168.2.1~~	~~192.168.2.2/24~~	~~10~~


The Internet
192.168.10.0/24
Using 20 Addresses
.10.1
.10.2
Router 1
.1.1
.2.1
.1.2
Router 4
.40.1
.3.2
.2.2
Router 2
.20.1
Using 6 Addresses
192.168.40.0/24
.3.1
Router 3
.30.1
Using 121 Addresses
192.168.30.0/24
192.168.20.0/24
Using 254 Addresses

Routing Table - Router 3

Network ID	Gateway	Interface	Metric
0.0.0.0/0	192.168.3.2	192.168.3.1/24	10
192.168.30.0/24	192.168.30.1/24	192.168.30.1/24	10
~~192.168.20.0/24~~	~~192.168.3.2~~	~~192.168.3.1/24~~	~~10~~
~~192.168.40.0/24~~	~~192.168.3.2~~	~~192.168.3.1/24~~	~~10~~
~~192.168.10.0/24~~	~~192.168.3.2~~	~~192.168.3.1/24~~	~~10~~


The Internet
192.168.10.0/24
Using 20 Addresses
.10.1
.10.2
Router 1
.1.1
.2.1
.1.2
Router 4
.40.1
.3.2
.2.2
Router 2
.20.1
Using 6 Addresses
192.168.40.0/24
.3.1
Router 3
.30.1
Using 121 Addresses
192.168.30.0/24
192.168.20.0/24
Using 254 Addresses

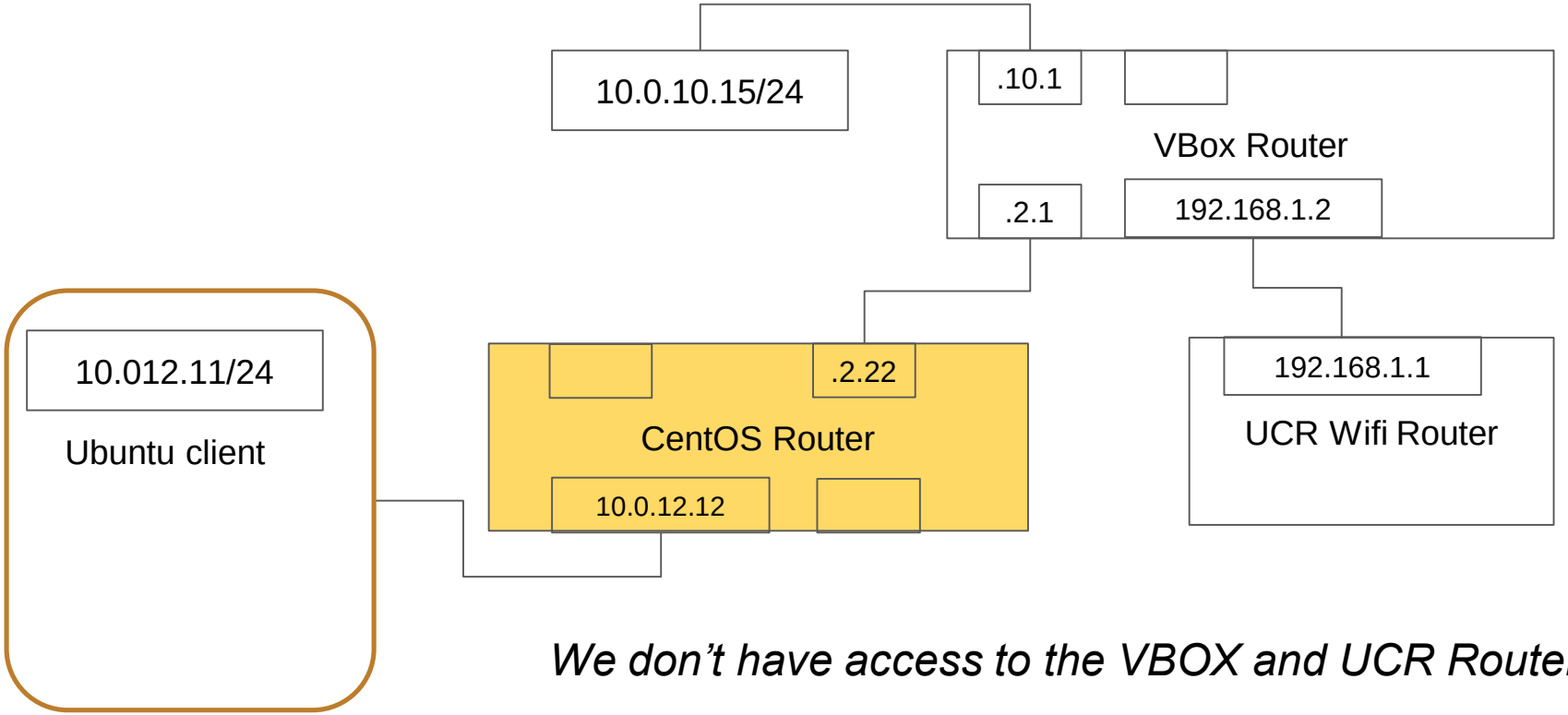
Routing Table - Router 4 (Exercise)

Network ID	Gateway	Interface	Metric
			10
			10
			10
			10
			10

Routing Table - Router 4

Network ID	Gateway	Interface	Metric
0.0.0.0/0	192.168.1.1	192.168.1.2/24	10
192.168.40.0/24	192.168.40.1/24	192.168.40.1/24	10
192.168.30.0/24	192.168.3.1	192.168.3.2/24	10

Example: setting up static routing for a network



We don't have access to the VBOX and UCR Routers

Example: steps to provide external access

- To use the Linux system as a router, ip forwarding should be enabled
- ip forwarding refers to capability of redirecting ip packets:
    - sysctl -w net.ipv4.ip_forward=1
    - sysctl -p /etc/sysctl.conf
    - This configuration would override the value stored in **/proc/sys/net/ipv4/ip_forward**
- We need to add the routes
    - A simple default route suffices: sudo ip route add default via dev 10.0.2.1

Example: **Network Address Translation (NAT)**

- Outside routers do not know about our internal structure!
  - The router will route the traffic but we will not get any responses back!
- NAT allows us change the sender address to the router address
  - The outside routers know where to send the traffic for the router address
- The command is:
  - iptables –t nat -A POSTROUTING -o enp0s3 -j SNAT --to-source 10.0.2.22

Routing protocols

- Routing protocols simplify the configuration process by automatically compiling routing tables
- Most common protocols are:
    - RIP: simple distance-vector protocols that use hop counts as a cost metric
    - EIGRP: another distance vector protocol that is designed to avoid looping problems
    - OSPF: most popular dynamic routing protocol, only usable on internal private networks, analogous to STP in L2

Open Shortest Path First (OSPF)

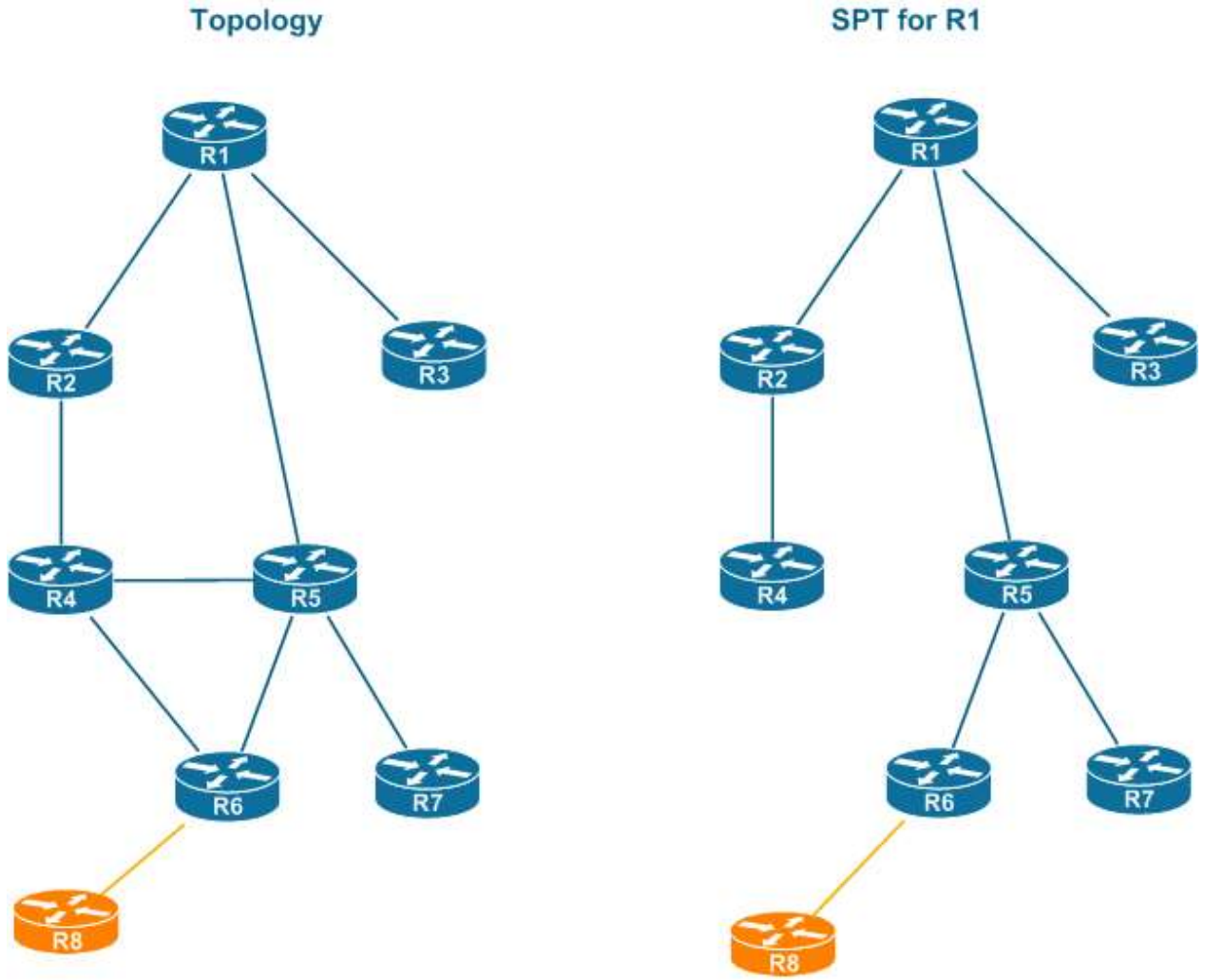
- Most popular dynamic routing protocol, only usable on internal private networks, analogous to STP in L2
- Designed for networks using variable length CIDR addresses
- It is able to converge on a loop-free topology quickly (seconds)
- Can handle any topology structure and allows for authentication

Terminology

- **Area**: way to segment networks in OSPF using a 32 bit ID
- **Neighbor**: connected router running OSPF in the same area
- **Adjacency Database**: table of all OSPF connections that are neighbors
- **Router ID**: unique ID of a router within an area
- **(Backup) Designated Router**: routers which hold global topology view (all routers must form an adjacency to these), they are elected by priority

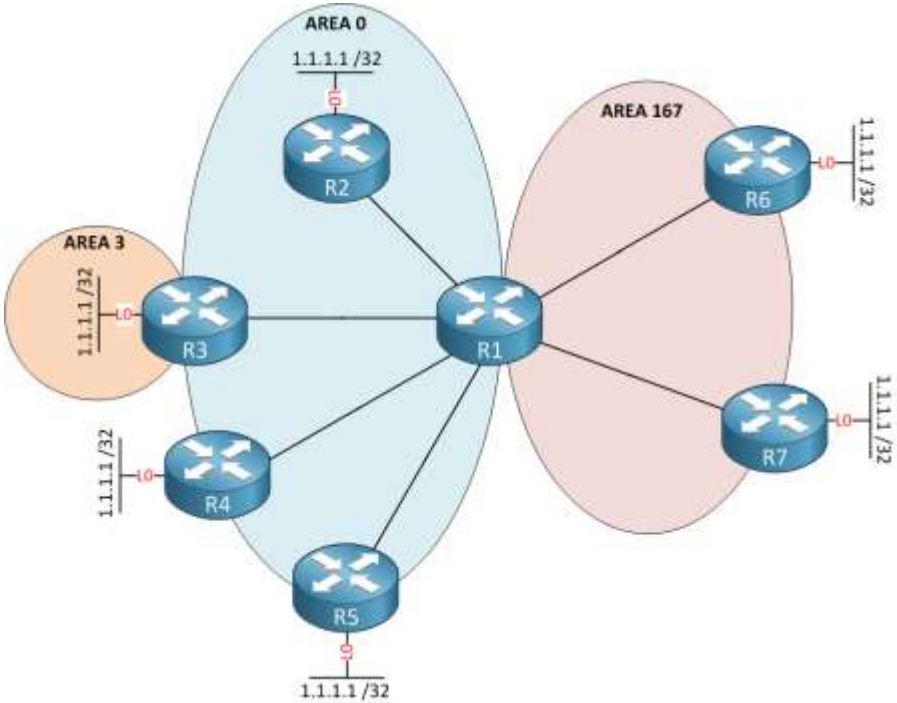
OSPF Algorithm

1. Neighbor Discovery:
    a. Use L2 broadcast “hello” messages to identify “adjacent” neighbors
    b. These routers must interface on the same subnet, have different IDs, be in the same area, and have the same authentication parameters
2. Topology Database Exchange:
    a. Send **Link State Advertisements** (LSA) onto the network which contains a router ID, list of router interfaces, and list of neighbors on each interface
    b. Routers store this information into the **Link State Database** (LSDB), which should be the same for all routers in the area
3. Route Computation
    a. Use a **Shortest Path First** (SPF) algorithm (equivalent to Dijkstra’s) based on LSDB information
    b. Update the routing table with the routes calculated using SPF


Topology
R1
R2
R3
R4
R5
R6
R7
R8
SPT for R1
R1
R2
R3
R4
R5
R6
R7
R8

Areas

- Breaking our network into smaller areas allow for a number of benefits when running OSPF
  - Smaller LSDBs for each router in the area
  - Reduction in the amount of LSA traffic, since it won't traverse area boundaries
  - Quicker SPF calculations (mostly because of the above)

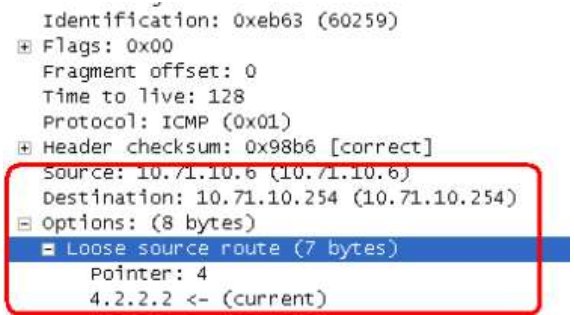


Security Issues at layer 3

- Security is a multi-layer concept
- In a network, a server/client could be vulnerable at one or multiple layers
- Vulnerabilities in layer 3 can have different effects:
    - Bypassing firewall rules
    - Denial of services
- It is important to understand that there is neither authentication nor encryption at layer 3
    - VPN tunneling provides both for layer 3

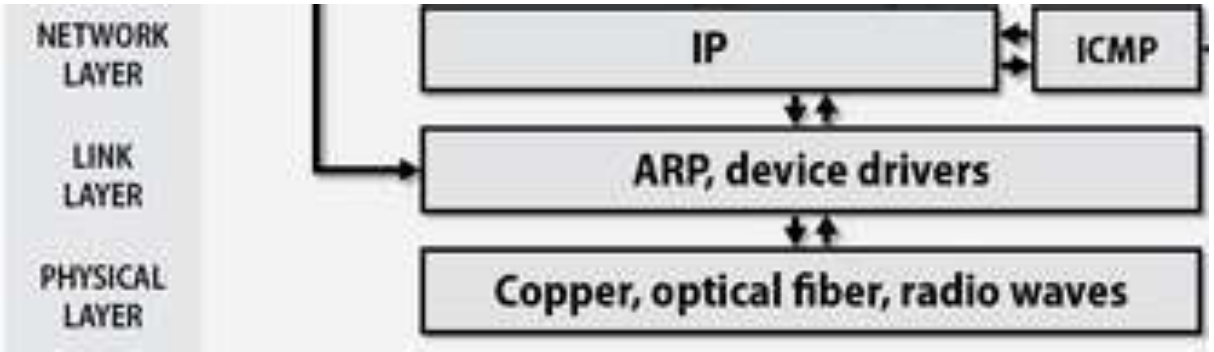
Routing issues

- IP forwarding: unless you perform routing IP forwarding should be disabled
  - Otherwise, an attacker can trick your router into routing their packets and possibly bypass network scanners and packet filters
- Source routing: IP protocol allows the sender to choose their route to the destination
  - Through Strict Source Route (SSR) and Loose Source Route (LSR) header options
  - It can be misused to bypass firewalls



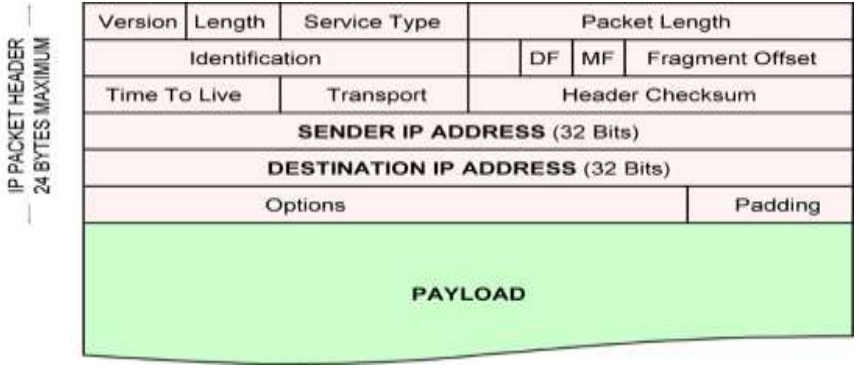
ICMP redirects

- Internet Control Message Protocol (ICMP) is a supporting protocol in the Internet protocol suite
- The router can inform senders of particular problems by sending “ICMP redirects”
    - The message says you should not send packets for host x to me, send it to y
- In theory, the recipient might adjust its routing table to reflect the change



IP spoofing

- Sender IP is usually set by the kernel
- An attacker can craft a packet with a sender IP other than their own
    - Firewall might permit the packet from the forged address
- IP spoofing is mainly used for DDOS attacks
    - Combined with source routing can completely bypass L3 IP filtering



Questions?

Additional Resources

Packet Guide to Routing and Switching (Chapter 5 and 6)