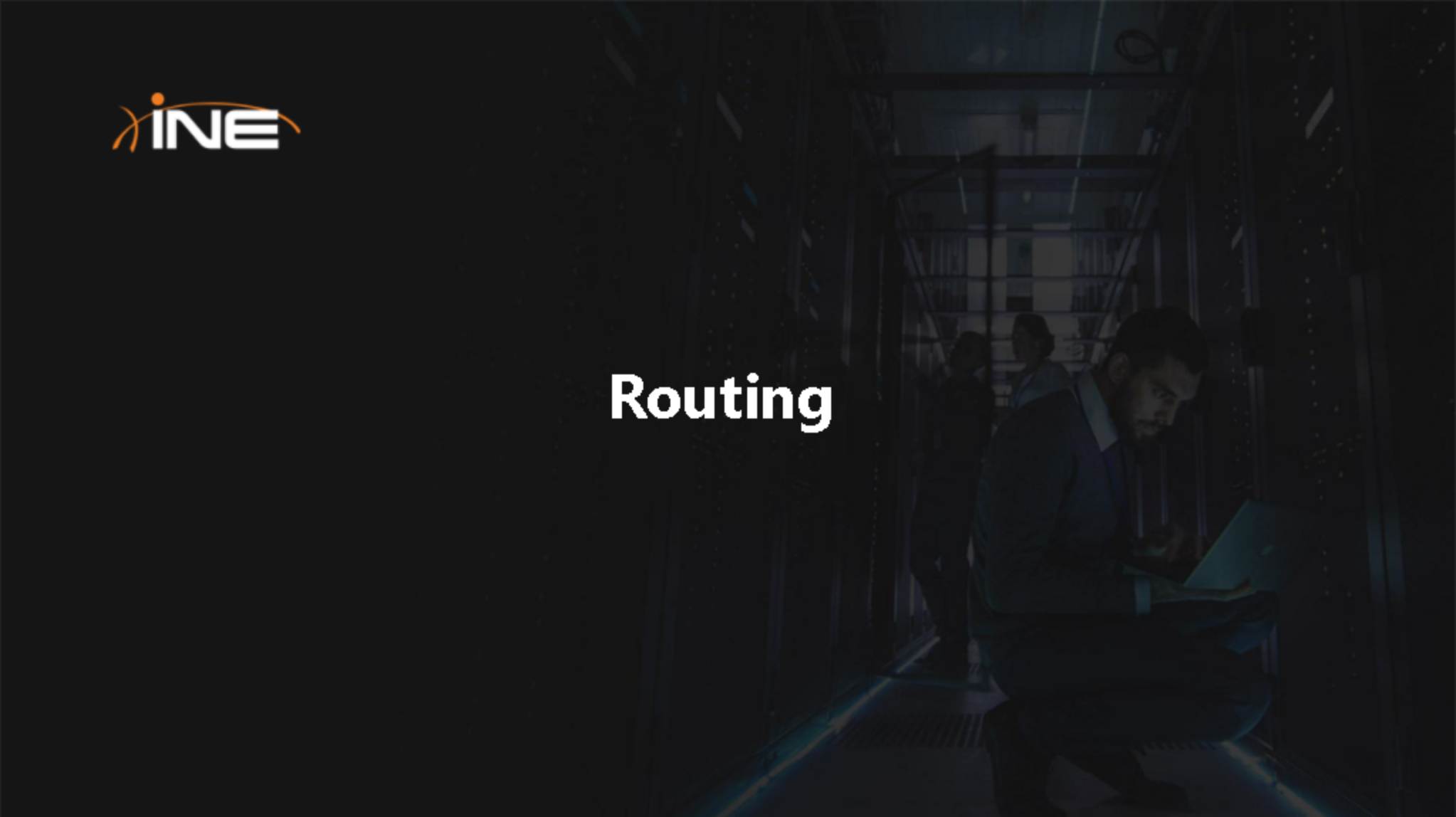
Routing



2.3 Routing

+ **How does this support my pentesting career?**

  - Understanding routing protocol attacks
  - Performing network traffic inspection

2.3 Routing

- Addressing devices is just half of the work needed to reach a host. Your packets need to follow a valid **path** to reach it.

- **Routers** are devices connected to different networks at the same time. They are able to forward IP datagrams from one network to another. The forwarding policy is based on **routing protocols.**

2.3 Routing

- Routing protocols are used to determine the best path to reach a network. They behave like a postman who tries to use the shortest path possible to deliver a letter.

- A router inspects the destination address of every incoming packet and then forwards it through one of its interfaces.

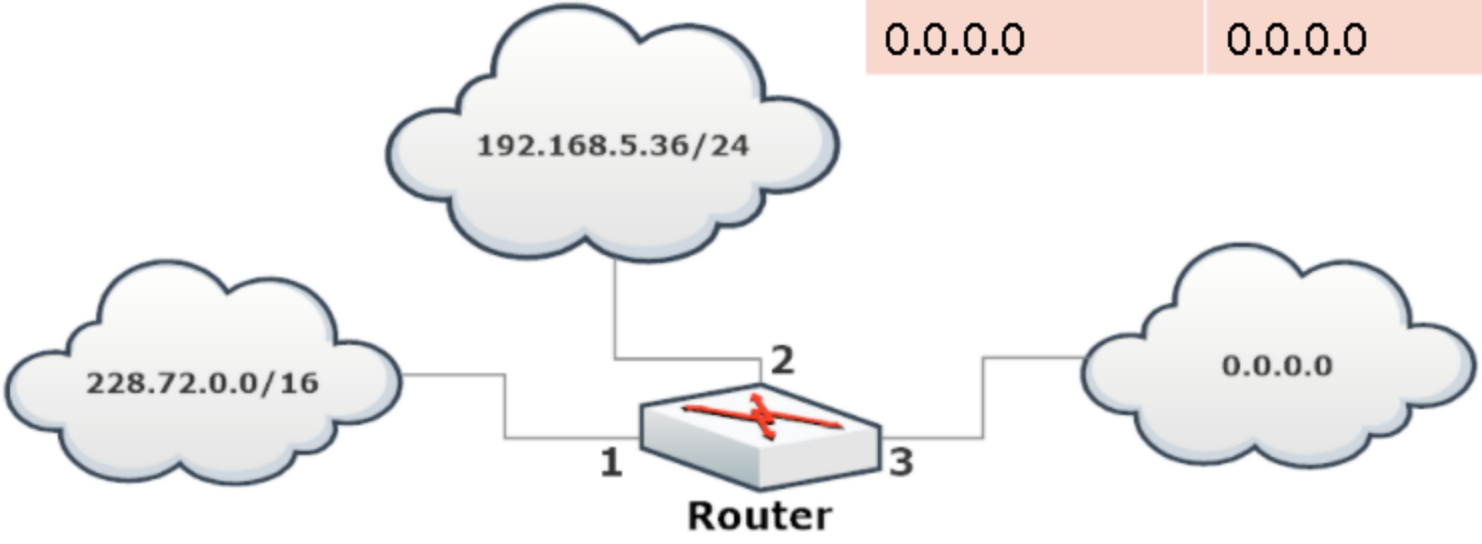
2.3.1 Routing Table

- To choose the right forwarding interface, a router performs a lookup in the **routing table**, where it finds an IP-to-interface binding.

- The table can also contain an entry with the **default address** (0.0.0.0). This entry is used when the router receives a packet whose destination is an *unknown network*.

2.3.1.1 Routing Table Example

IP	Netmask	Interface
228.72.0.0	255.255.0.0	1
192.168.5.0	255.255.255.0	2
0.0.0.0	0.0.0.0	3



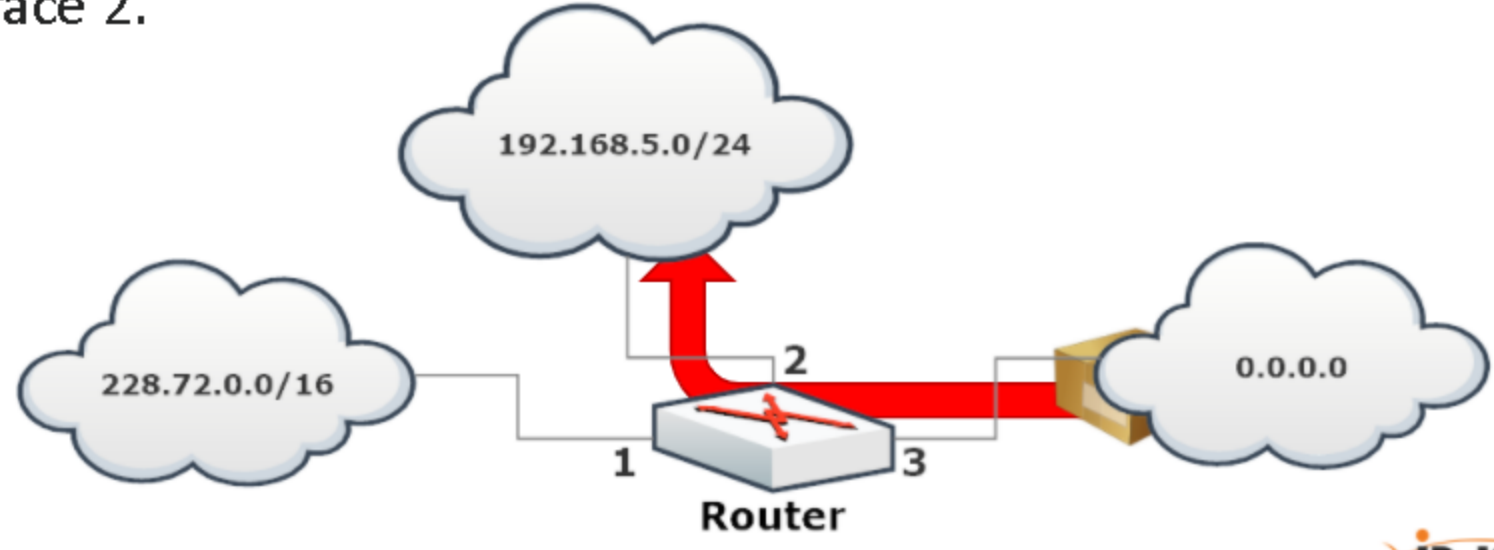
2.3.1.1 Routing Table Example

+ In this example, the routing table is made of three entries.
  - Interface 1 is used to forward the packets to 228.72.0.0/16.
  - Interface 2 is used to forward the packets to 192.168.5.0/24.
  - Interface 3 is used as the default route for packets whose destination does not match any other entry in the table.

2.3.1.1 Routing Table Example

EXAMPLE

+ A packet arriving on interface 3 for 192.168.5.3 is forwarded on interface 2.



2.3.1.1 Routing Table Example

- In fact, the first entry in the routing table does not match the destination network.

To: 192.168.5.3

IP	Netmask	Interface
228.72.0.0	255.255.0.0	1
192.168.5.0	255.255.255.0	2
0.0.0.0	0.0.0.0	3

2.3.1.1 Routing Table Example

- While the second does: `192.168.5.3` sits in the `192.168.5.0/24` network.

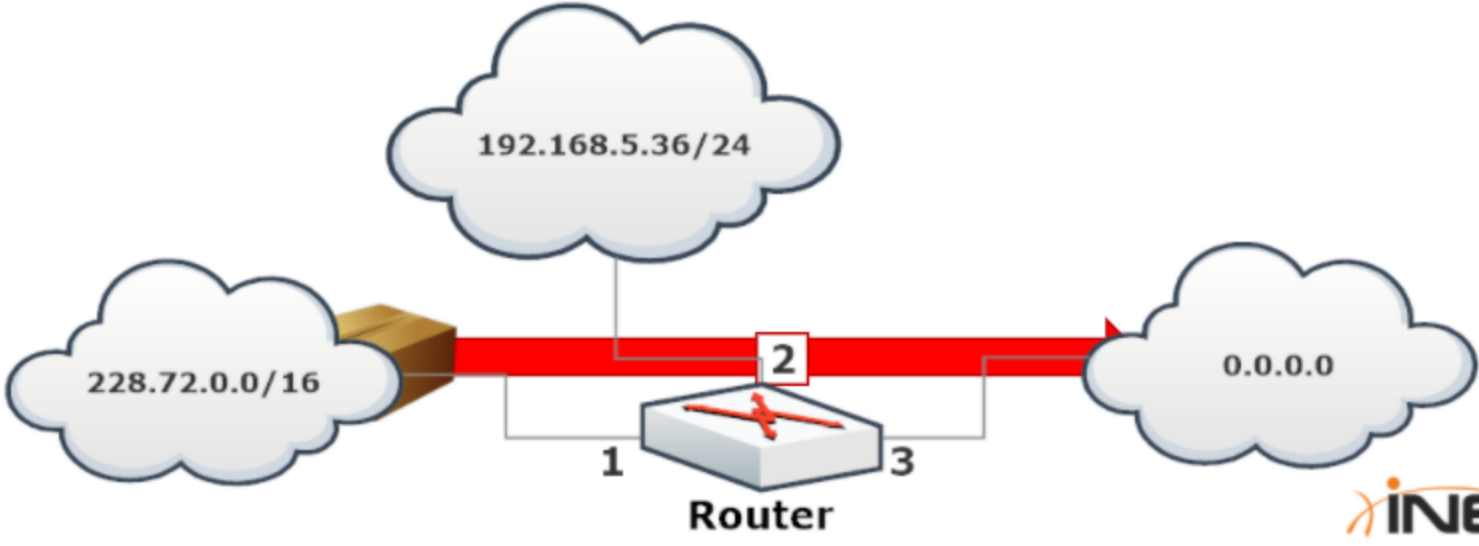
To: 192.168.5.3

IP	Netmask	Interface
228.72.0.0	255.255.0.0	1
192.168.5.0	255.255.255.0	2 ✓
0.0.0.0	0.0.0.0	3

2.3.1.2 Default Route Example

EXAMPLE

+ A packet arriving on interface 1 for 72.13.37.2 is routed through interface 3, the default route.



2.3.1.2 Default Route Example

- There is no matching entry, so the router forwards the packet through interface 3.

To: 72.13.37.2

IP	Netmask	Interface
228.72.0.0	255.255.0.0	1
192.168.5.0	255.255.255.0	2
0.0.0.0	0.0.0.0	3 ✓

2.3.2 Routing Metrics

- As in the real world, there could be more than a way to reach a destination.

- So, during path discovery, routing protocols also assign a **metric to each link**.

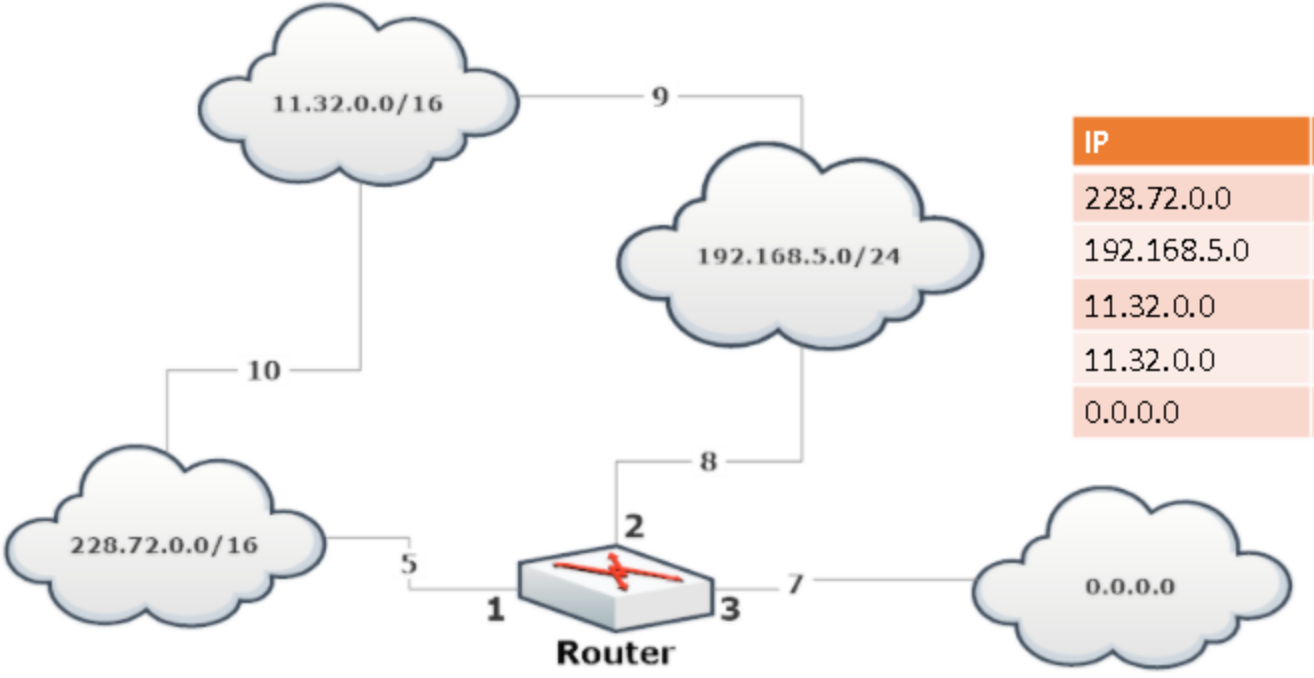
2.3.2 Routing Metrics

- This ensures that, if two paths have the same number of hops, the fastest route is selected.

- The metric is selected according to the channel's estimated bandwidth and congestion.

2.3.2.1 Routing Metrics Example

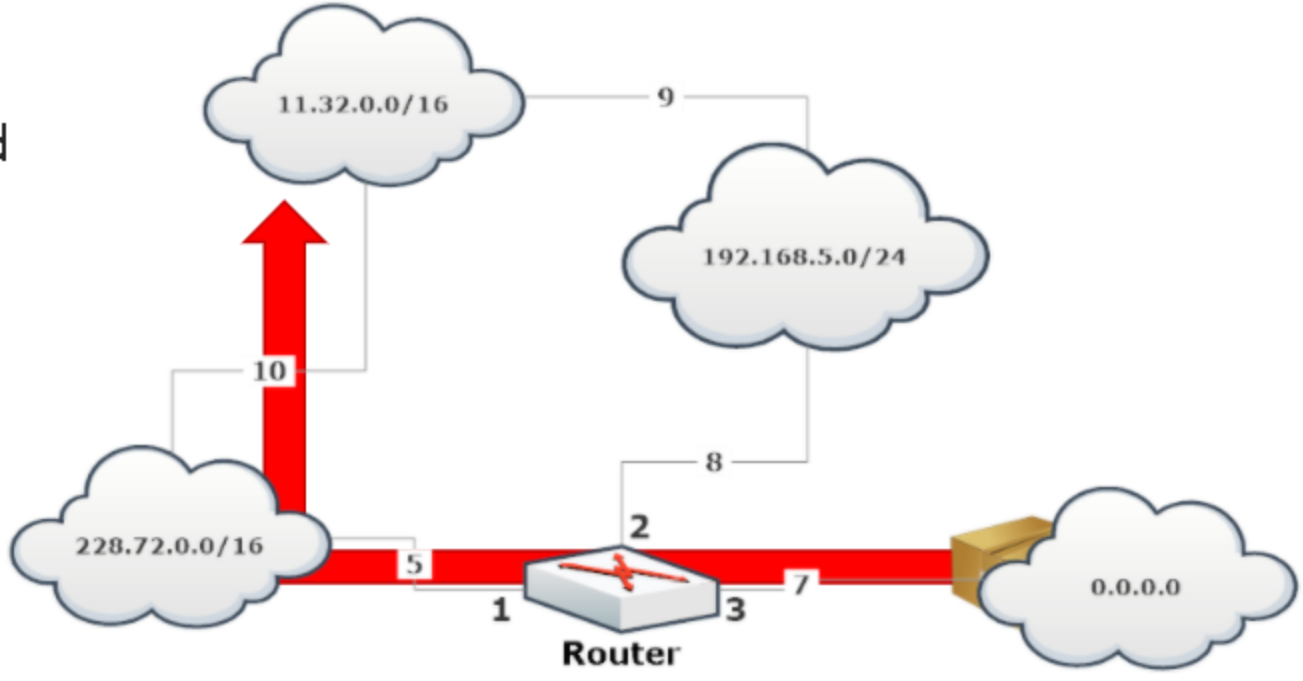
- Let's look at how routing decisions are made according to metrics.



IP	Netmask	Interface	Metric
228.72.0.0	255.255.0.0	1	5
192.168.5.0	255.255.255.0	2	8
11.32.0.0	255.255.0.0	2	17
11.32.0.0	255.255.0.0	1	15
0.0.0.0	0.0.0.0	3	7

2.3.2.1 Routing Metrics Example

- A packet arriving on interface 3 for 11.32.3.118 is routed through interface 1, as the metric for that route is 15.
- Routing through interface 2 would have a metric of 17.



2.3.3 Checking the Routing Table

- Routing tables are not only kept by routers; every host stores its own table.

- To check what they look like, you can use:
  - `ip route` on Linux
  - `route print` on Windows
  - `netstat -r` on OSX

2.3.3 Checking the Routing Table

EXAMPLE

+ Checking the routing table on a Linux box:

```
root@host:~# ip route
default via 192.168.51.1 dev eth0  proto static
192.168.51.0/24 dev wlan0  proto kernel  scope link  src 192.168.51.123
```

2.3.3 Checking the Routing Table

EXAMPLE

+ Checking the routing table on Microsoft Windows:

```
C:\Users\User>route print
===========================================================================
Interface List
 11...08 00 27 bf ac c8 ......Intel(R) PRO/1000 MT Desktop Adapter
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0        10.0.2.2        10.0.2.15     10
         10.0.2.0    255.255.255.0         On-link         10.0.2.15    266
```

2.3.3 Checking the Routing Table

EXAMPLE

+ Checking the routing table on Mac OSX:

```
User:~ user$ netstat -r
Routing tables

Internet:
Destination        Gateway            Flags        Refs      Use   Netif Expire
default            192.168.51.1       UGSc           13        0     en1
127                127.0.0.1          UCS             0        0     lo0
127.0.0.1          127.0.0.1          UH              1       16     lo0
169.254            link#4             UCS             0        0     en1
192.168.51         link#4             UCS             4        0     en1
192.168.51.1       58:6d:8f:e5:e:d2   UHLWIir        14       24     en1   1200
192.168.51.109     2:f:b5:4b:76:cf    UHLWIi          0        0     en1   1148
```