



COMPUTER SYSTEMS ENGINEERING
COMPUTER NETWORKS LAB

Report #1

Student:

AMEER ALKAM

ID:

1120217

Supervisor:

DR. IYAD TUMAR

Teacher Assistant:

ODAI SALMAN

Partners:

OMAR MUHTASEB - 1122010

SONDUS SAMARA - 1121775

March 28, 2016

Abstract

Network Addressing and Routing are essential pieces of any network, these two define which devices are connected to which networks (or sub-networks) and how to reach said devices. Addressing is achieved using the IPv4 and IPv6 addresses. Routing is divided into two categories, Static and Dynamic, where static routing is configured manually by the admin of the router, while dynamic routing uses specialized algorithms such as RIP, IGRP, or OSPF, to create routing tables, which are tables holding in their entries how the traffic should be directed to reach a specific sub-network/device. In the experiments reported here, we were exposed to the basic concepts, and elements, of networks, and we also simulated the behaviour of networks under static routing, as well as multiple dynamic routing algorithms, namely, RIP, IGRP, and OSPF, using CISCO's PacketTracer software.

Contents

I	Introduction	1
1	Interfacing defintions	1
1.1	The Ethernet interface	2
2	What is routing?	4
3	Administrative Distance	5
4	Static Routing	5
5	Dynamic Routing	5
5.1	Distance Vector Routing, RIP	6
5.1.1	IGRP	6
5.2	Link State Routing, OSPF	7
5.2.1	The higherarchy of OSPF	7
5.3	Summarization	8
6	The CISCO routers and IOS	9
II	Procedure	10
1	Interfaces - distributing IP's, and configuring routers	10
2	Static Routing	15
3	Dynamic Routing	15
3.1	RIP	15
3.1.1	IGRP	16
3.2	OSPF	17
III	Conclusions	20

Part I

Introduction

1 Interfacing definitions

Each device, on any network, uses a Network Interface Card (NIC) in order to connect to said network. And every NIC present on a network is assigned to one unique address, known as an IP address. No two devices are allowed, or can have, the same IP address. These IP addresses function on Layer-3 (Network layer) of the OSI, and the TCP/IP, models of networks, to communicate information and data between devices.

If a device has more than one NIC, eg. routers, it could have more than one IP, ie. one unique IP for each NIC, figure 1 shows an example router schema having multiple interfaces. These NIC's aren't necessarily required to be part of the same network, meaning that each NIC could be interfaced with a different network, this is an important idea, since networks are only allowed to connect to one another through boundary devices such as router, where these "boundary routers" have multiple interfaces, each connected to, and is part of, a different network, figure 2.

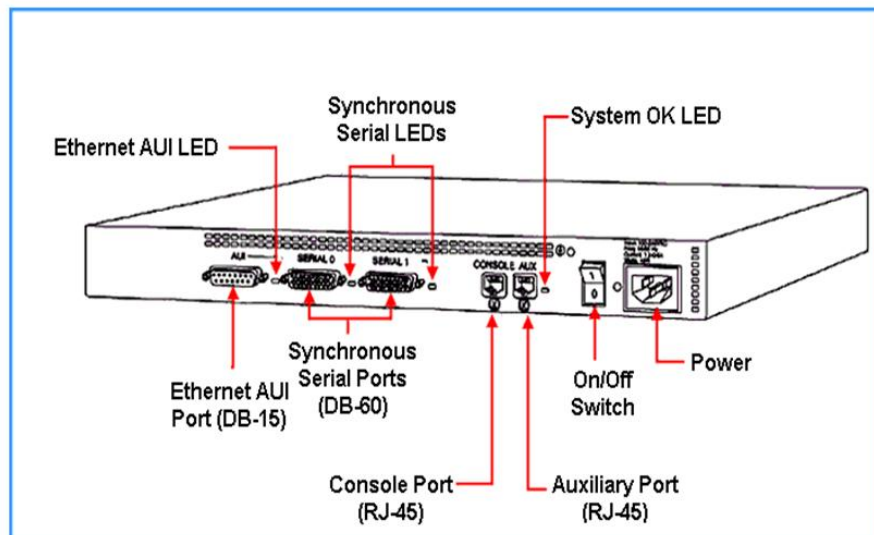


Figure 1: An example router schema, showing several interfaces, reference [2].

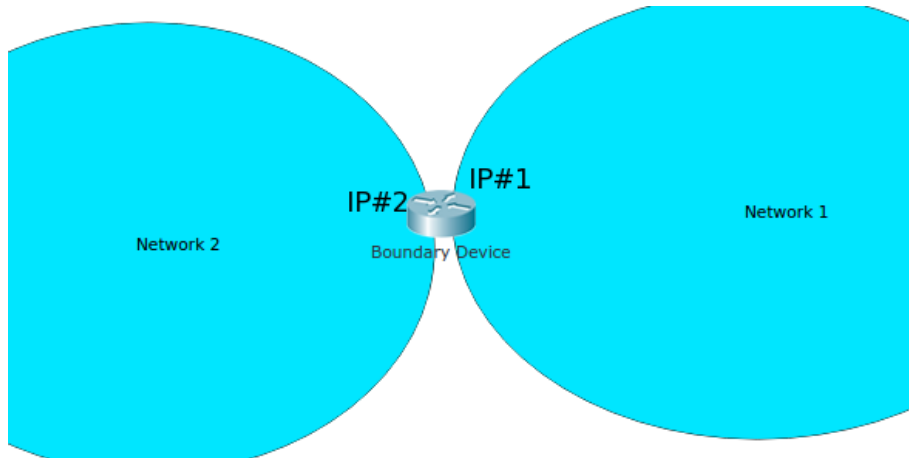


Figure 2: Two simplified networks connected via a boundary router. IP#1 belongs to Network 1, while IP#2 belongs to Network 2. IP#1 and IP#2 are connected each to it's own NIC, and are unique to each network it's part of.

1.1 The Ethernet interface

One of the most widely used standards for connecting devices in LANs, standard IEEE802.3 Ethernet, the standard was introduced in 1980 and standardized by the IEEE organization in 1983.

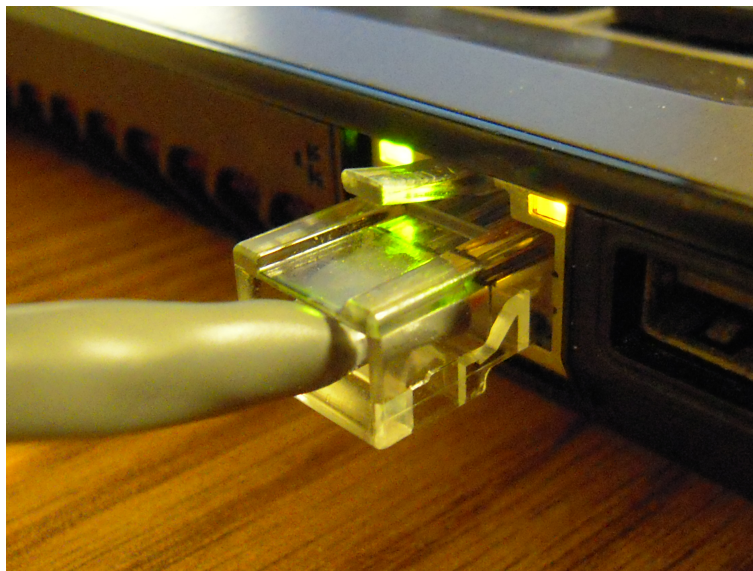


Figure 3: A Cat 5e connection on a laptop, used for Ethernet, reference [4].

We focus, in our experiments, on the types of cables used by the Ethernet standard, while the original Ethernet cable introduced in 1980 used *coaxial cables* as a shared medium, the newer more modern interfaces uses *twisted pair* and *fiber optics* links in conjunction with hubs and switches, figure 4 shows an Ethernet cable head. We note that there are three types of twisted pair cables, the *cross-over* cables used to connected PC's directly together, and the *straight-through* cables used to connect PC's to switches and other network devices, the third one is *roll-over* cables used to connect a router/switch to a PC through the console port for management purposes.



Figure 4: 8P8C modular connector, commonly referred to as RJ45, used for the Ethernet standard, reference [4].

RJ45 cables, the most common form of cables used for Ethernet, have 8 pins, figure 5 show how the pins are layed out between two peers in the three types of the cables. We notice that straight-through and cross-over links use only pins 1, 2, 3, and 6.

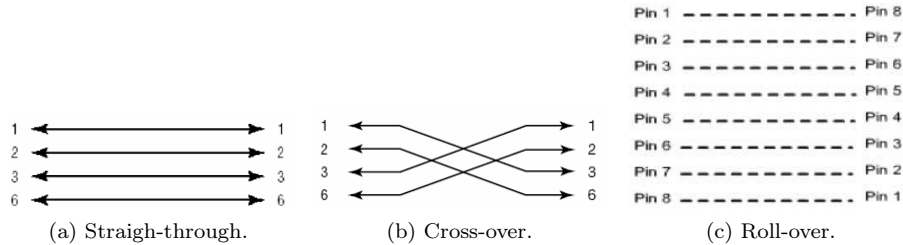


Figure 5: The pin layout of the three types of RJ45 cables.

2 What is routing?

Routing is the process in which Layer-3 devices, such as routers, determine which route, or path, traffic through a network must go, in order to achieve connectivity between network constituents.

ROUTING is the basis on which FORWARDING, which is the process where routers and other Layer-3 devices send packets of data they receive along a certain path, connection, or interface, relies on. Routers create what is known as *routing*, or *forwarding*, *tables*, which hold information regarding which link, interface, or path, is used to reach which devices, identified by their IP's, figure 6 shows how a routing table typically looks from within a routers CLI.

```

RouterO
Physical | Config | CLI |
IOS Command Line Interface

Router>show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    193.167.0.0/24 is directly connected, Serial2/0
O    193.167.1.0/24 [110/128] via 193.167.0.1, 01:08:53, Serial2/0
      [110/128] via 193.167.2.2, 01:08:53, Serial3/0
C    193.167.2.0/24 is directly connected, Serial3/0
O IA 193.168.0.0/24 [110/128] via 193.167.0.1, 01:09:13, Serial2/0
O IA 193.168.1.0/24 [110/128] via 193.167.0.1, 01:09:13, Serial2/0
O IA 193.168.2.0/24 [110/192] via 193.167.0.1, 01:09:13, Serial2/0
O IA 193.168.3.0/24 [110/129] via 193.167.0.1, 01:09:13, Serial2/0
O IA 193.168.4.0/24 [110/129] via 193.167.0.1, 01:09:13, Serial2/0
O IA 193.169.0.0/24 [110/192] via 193.167.2.2, 01:08:53, Serial3/0
O IA 193.169.1.0/24 [110/128] via 193.167.2.2, 01:08:53, Serial3/0
O IA 193.169.2.0/24 [110/128] via 193.167.2.2, 01:08:53, Serial3/0
--More--
Copy Paste

```

Figure 6: Example routing table, using PacketTracer.

Routing can be divided into two categories, which we'll get back to in the other sections:

Static Routing which requires a system admin to create, and maintain, the routing tables of a network's routers.

Dynamic Routing which uses specialized algorithms to create, and maintain, said routing tables.

3 Administrative Distance

Administrative Distance (AD) is a measure of *trustworthiness* of the routing information received by the router, it is a number between 0 and 255, where the lower numbers have the higher trustworthiness.

When a router receives two, or more, advertisements or updates at the same time regarding the same remote network, then the router first checks the administrative distance, the router with the lower AD is placed in the routing table, if the updates have the same AD number, then the metric used by the protocol in use. When the AD numbers and the metric used are equal, then the router in most cases would balance the load between the connections.

Typically, an AD number of 0 is given to the directly connected devices, and an AD number of 1 is given to routes statically configured.

4 Static Routing

The most basic form of routing, in which the routing table is constructed manually by the network admin. The simplicity and cost efficiency of this method helps it work quite well for small sized networks, but *scalability* is a major issue here, since any newly added device needs to have its routing entry manually added, and any changes made to the network would require the admin's intervention to modify the routing entries in the whole network, this can easily turn into a tedious, not to mention *inefficient*, way to run a large network!

5 Dynamic Routing

Dynamic routing uses specialized algorithms to create and update the router's routing table. These algorithms aim to minimize the cost of connecting two devices, this is accomplished by using one of two general measures, link state and distance vector.

Link-state is a measure of cost that uses the *accumulative link cost*, between two devices, arising from the links, needed to be passed through, with other devices in between. Examples of it are the Routing Information Protocol (RIP) and the Interior Gateway Routing Protocol (IGRP).

Distance-vector is another measure of cost that uses the number of devices, or *hops*, between two devices, needed to be passed before reaching the destination. An example of which is the Open Shortest Path First (OSPF) protocol.

The most famous examples of routing algorithms are RIP, OSPF, and BGP. In our experiments and simulations we tested RIP, OSPF, and IGRP, which is a CISCO proprietary modified version of RIP. While the three types we tested are *Interior Gateway Protocols*, BGP is an *Exterior Gateway Protocol* used to route the entire Internet.

Although Dynamic routing is easier to use and more adaptable to change than static routing, it does have a toll in the bandwidth of the network, were it gets flooded with traffic with each update, and in CPU processing at the routers.

5.1 Distance Vector Routing, RIP

In distance vector routing algorithms Bellman-Ford algorithm is typically used, where each router has knowledge of it's direct neighbours And, periodically, each router broadcasts its routing information to its neighbours. After time passes, each router, node, will have knowledge of the entire network, and can calculate it's routing table based on the network information.

With each advertisement, each router sends the entire content of it's routing table to its neighbours, which in turn combine these info with their own, updating their routing entries, this is called *routing by rumor*. The first thing RIP checks for when receiving routing information is the AD number of the routes, if two routes lead to the same network, have the same AD number and the same cost (number of hops to get to), then RIP balances the load on the routes by performing *round-robin*. RIP is capable of load-balancing up to 6 links at the same time.

At max there can be up to 15 hops between two devices in RIP, any more than that means that the devices can't "see" each other, a number of hops of 16 is treated as infinity in RIP.

5.1.1 IGRP

IGRP was a proprietary modification of RIP, introduced by CISCO, mainly, to overcome the number of hops limitations imposed by RIP.

RIP was limited, as stated before, to a maximum of 15 hops, also RIP can only account for a single metric of routing. In contrast, IGRP uses a formula compsed of multiple routing metrics, which are bandwidth, delay, load, and reliability, to infere which route is better. It also increased the number of hops significantly to a maximum of 255, default configuration sets it to 100.

5.2 Link State Routing, OSPF

In link state routing algorithms each router has total knowledge of all the links, and their costs, in the entire network, and uses shortest path algorithms, typically *Dijkstra's*, to determine the shortest path to all other devices.

OSPF is the most widely used interior gateway protocol in large enterprise networks. In contrast to RIP, the advertisements in OSPF, the *link-state advertisements* or *LSA's*, are sent to *all* other routers in the *same area*, we'll discuss the notion of areas later on.

OSPF routes packets *solely* within a single *routing domain*, such as an autonomous system. It uses the data from all routers to create a topological map of the *entire* network. It can also detect any failures or updates to any link, and quickly update the routing tables within seconds!

OSPF does not use, the Transport Layer to communicate information, that is, it doesn't rely on TCP nor UDP to send the information required to other routers. Rather it encapsulates it's data in IP *datagrams* and implements it's own error detection/correction functions, this further distinguishes OSPF from other routing protocols such as RIP, and even BGP.

The messages exchanged by routers under OSPF carry all kinds of information, but crucially, and for two routers to be considered "neighbours", four bits of information must be common, these are the *hello and dead timers*, the *network mask*, the *area ID*, and the *authentication password*.

OSPF is preferred as a routing algorithm choice when the network is required to be divided into areas and zones.

5.2.1 The hierarchy of OSPF

OSPF by its design, split the network into multiple *areas*, or *zones*. This allows the network to be managed more efficiently and easily. Each area is given a unique ID, the backbone of the network, which all other areas connect to, is known as *area-0*, areas are only allowed to connect to one another via an *area border router (ABR)*. The multiple of areas composing a large network can be viewed as a complete independent entity from the outerworld, known as an *Autonomous System (AS)*. AS's connect to the outer world via an *Autonomous System Boundary Router (ASBR)*.

Autonomous System (AS)

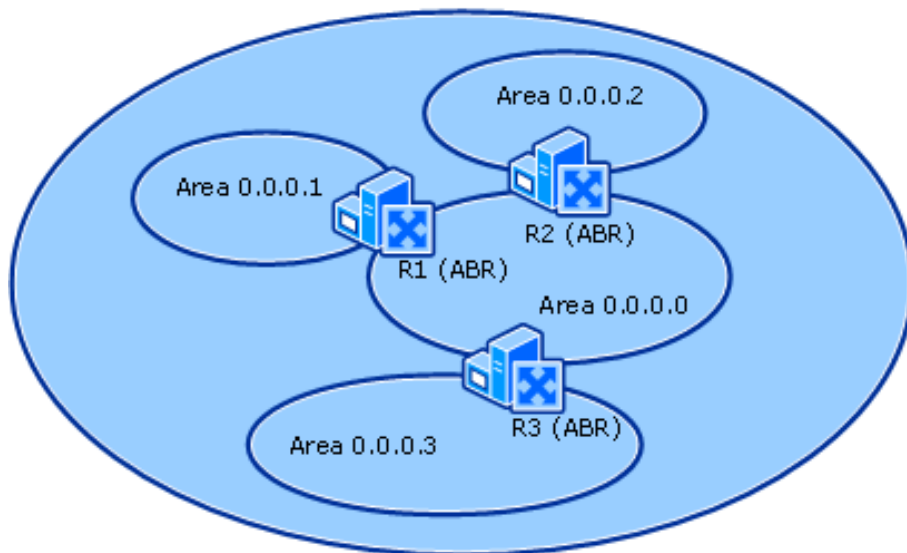


Figure 7: Example of a hierarchical autonomous system, reference [8].

5.3 Summarization

Summarization is a process to reduce the bandwidth consumption when routing protocols start advertising their info, specially in OSPF where the entire network would get flooded with traffic. It works by merging subnetworks into larger ones when being advertised, by using a larger subnet mask, able to cover the subnetworks being merged.

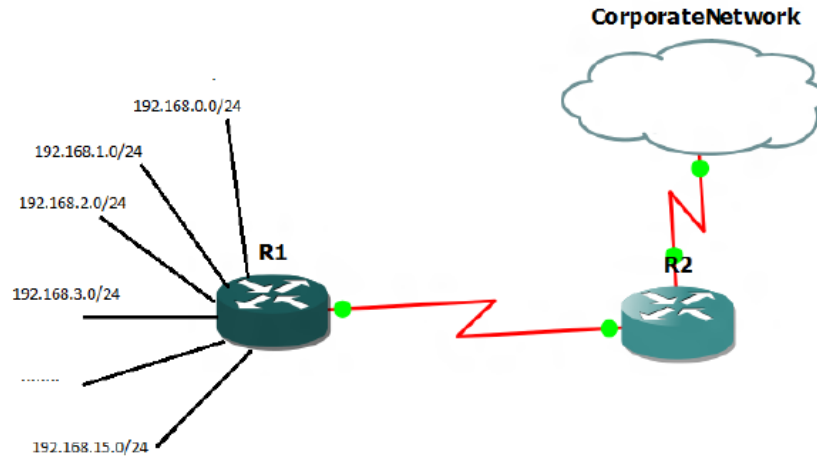


Figure 8: An example of an summarization scenario.

For example, in figure 8, router R1 can either send the information of the 16 networks connected to it, one by one, or it can send out one message informing the network that the larger, as if it has one single network connected to it, 192.168.0.0/20 network belongs to it, saving bandwidth and traffic, as well as time.

6 The CISCO routers and IOS

The configuration of a CISCO router is achieved via a command line interface, with the network admin connected to the router via a *serial console* port, an *auxiliary* port, or using the *telnet* program. The routers are run by a software called IOS, acronym for the *Internetwork Operating System*, which is responsible for providing the tools and functions necessary to run and manage the various routing algorithms and protocols, as well as to secure the network, and manage the traffic flow through routers running it.

Part II

Procedure

The following procedure takes place in CISCO's PacketTracer network simulation software.

1 Interfaces - distributing IP's, and configuring routers

Let's begin our focus on the topologies by giving each NIC, for each device, a unique IP address, making sure to distinguish each unique network with a different network ID.

Let's start distributing ID from the hosts, this is simply achieved by going to the IP configuration settings for each host, this is achieved by choosing the device, going to the "Desktop" tab, and choosing IP config, as shown in the following figure 9.

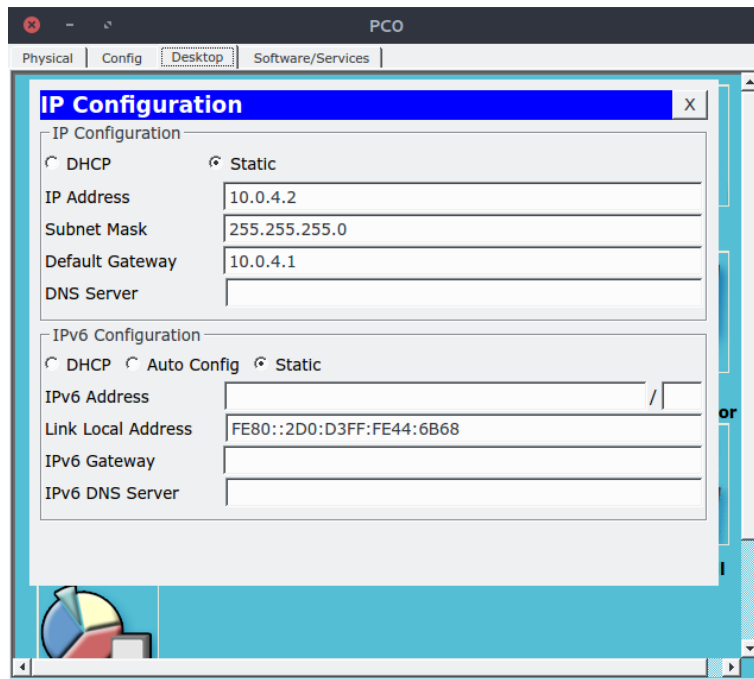


Figure 9: IP configuration panel, for the generic PC in PacketTracer.

We then simply fill in with the IP address of choice, that follows the network we're constructing, give it the appropriate subnet mask, and a default gateway,

which is the IP address of the subnet's boundary router, from the NIC that's part of the network. This is repeated for all hosts in all the networks being built.

Doing things for the routers is a bit different, since each router must be configured from the command line, to be properly exposed to the settings being made, to achieve this, we go through two steps, the first is we specify the NIC we're configuring, since routers have more than one NIC, and after that we give it the desired IP address.

Before we begin working with router interfaces, we first must enter the configuration mode for the router, this is achieved by first opening the router, choosing the *CLI* tab, a then typing the following commands, first `'en'`, to enable modifying the router, followed by `'conf t'` to enter configuration mode.

Now that we can configure the router, let's take a look at the commands for giving the interfaces their IP's,

`'int <interface name>'`, this commands chooses the interface needed, we specify the interface by it's name, or symbol, eg. Fa0/0 for Fast Ethernet port 0/0.

`'ip address <desired IP> <subnet mask>'`, this command assign the IP to the NIC.

Commonly the NIC would be shut down when first starting a router, so it is advised to start it up using the command `'no shut'` while being in the same interface config.

One of the interfaces available on routers, is *serial interface*, which is represented by the red lightning like line connecting routers, this interface requires a couple of more commands intended to configure the serial communication bases, the commands are first

```
'clock rate <desired clockrate in Hz>'
```

to configure the clock rate of the interface, followed by

```
'bandwidth <desired bandwidth in kiloHz>'
```

to configure the bandwidth of the connection.

Following is a simple topography, of 5 networks, and how to configure the IP's for all devices in it.

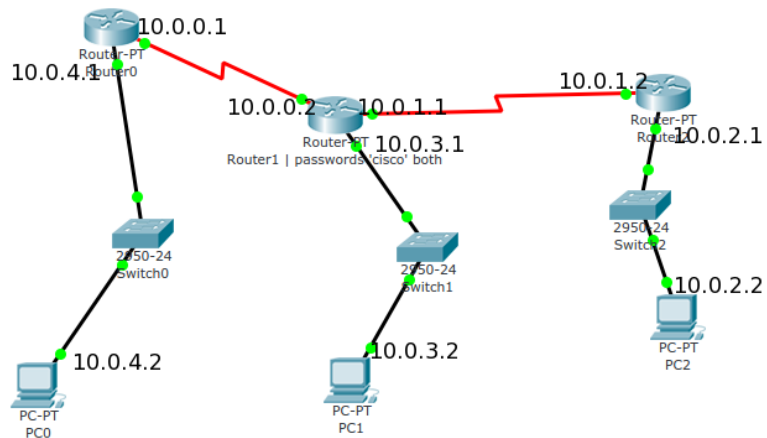


Figure 10: Simple topography, distributing IP's. Each device has the IP assign to it's interface, all have subnet mask /24.

Configuring the routers one by one would be as show in table 1.

For Router 1, we also configure a password, to demonstrate how it is set up, we can set up two passwords for a CISCO router, one for logging in remotely, using the likes of *telnet*, and another to enable enabling the configuration of it remotely, the commands to do so are as follows, first we enter the configuration mode of the router, then use the command 'line vty 0 4' to establish a console password, followed by 'password <desired password>' to set the pasword, if remote configuration is desired we can follow up with the command 'enable password <desired password>'. We configured the second router with a password as follows.

```

1 >line vty 0 4
2 >password hello
3 >enable password cisco

```

Figure 11 shows logging in to the configuration mode of the second router using telnet command.

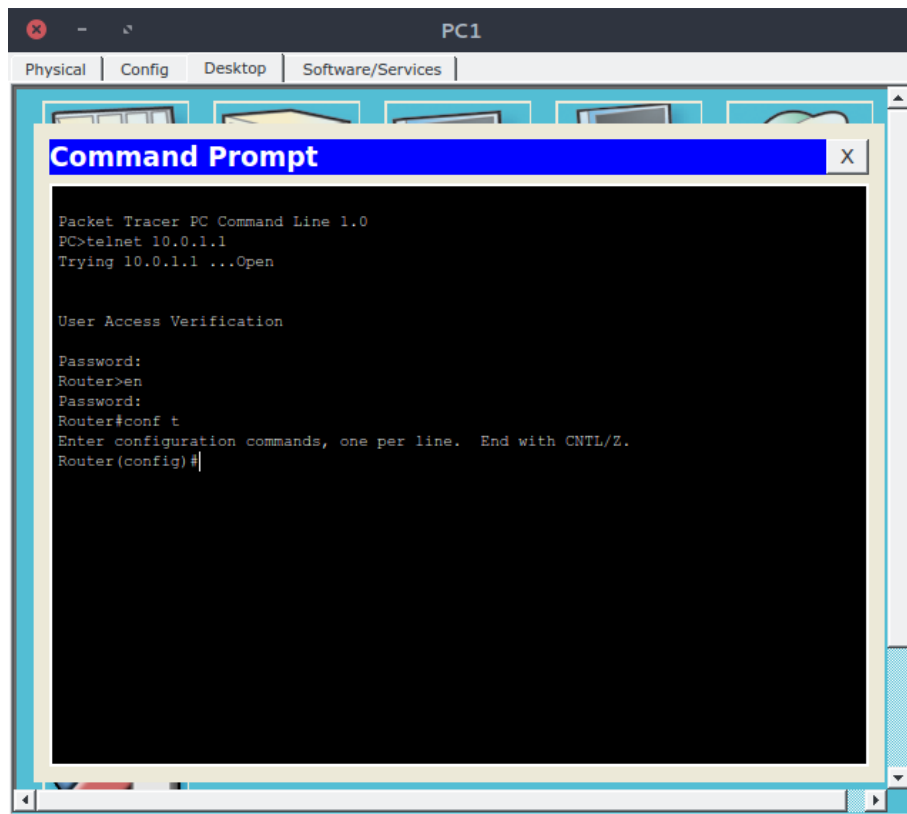


Figure 11: Accessing the configuration mode of Router 1 remotely.

Router	Commands
0	<pre> >en >conf t >int se2/0 >ip address 10.0.0.1 255.255.255.0 >clock rate 64000 >bandwidth 64 >no shut >int fa0/0 >ip address 10.0.4.1 255.255.255.0 >no shut </pre>
1	<pre> >en >conf t >int se2/0 >ip address 10.0.0.2 255.255.255.0 >clock rate 64000 >bandwidth 64 >no shut >int se2/1 >ip address 10.0.1.1 255.255.255.0 >clock rate 64000 >bandwidth 64 >no shut >int fa0/0 >ip address 10.0.3.1 255.255.255.0 >no shut </pre>
2	<pre> >en >conf t >int se2/0 >ip address 10.0.1.2 255.255.255.0 >clock rate 64000 >bandwidth 64 >no shut >int fa0/0 >ip address 10.0.2.1 255.255.255.0 >no shut </pre>

Table 1: Commands used to configure the routers in the topology of figure 10.

Configuring the hosts is done from the IP configuration setting from the Desktop tab as demonstrated in the previous figure 9.

2 Static Routing

The command for static routing is

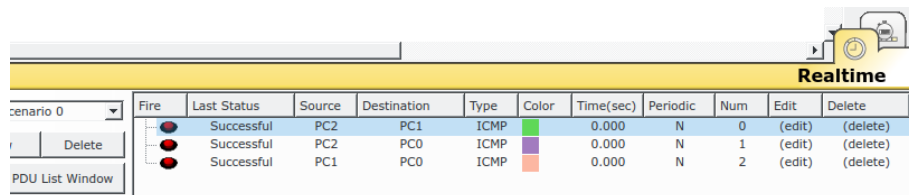
```
1 'ip route <destination network ID> <subnet mask> <next hop>'
```

To enable static routing on the previous topology, figure 10, we can use the following commands for each router.

Router	Commands
0	>ip route 10.0.3.0 255.255.255.0 10.0.0.2 >ip route 10.0.2.0 255.255.255.0 10.0.0.2
1	>ip route 10.0.4.0 255.255.255.0 10.0.0.1 >ip route 10.0.2.0 255.255.255.0 10.0.1.2
2	>ip route 10.0.3.0 255.255.255.0 10.0.1.1 >ip route 10.0.4.0 255.255.255.0 10.0.1.1

Table 2: Commands used to configure static routing in the topology of figure 10.

We can see that the configuration worked by sending messages from all hosts to each other, figure 12.



The screenshot shows a 'Realtime' window in a network simulation. It contains a table with the following columns: Fire, Last Status, Source, Destination, Type, Color, Time(sec), Periodic, Num, Edit, and Delete. The table lists three successful ICMP events:

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC2	PC1	ICMP	green	0.000	N	0	(edit)	(delete)
	Successful	PC2	PC0	ICMP	purple	0.000	N	1	(edit)	(delete)
	Successful	PC1	PC0	ICMP	orange	0.000	N	2	(edit)	(delete)

Figure 12: The success in connecting all hosts using static routing.

3 Dynamic Routing

3.1 RIP

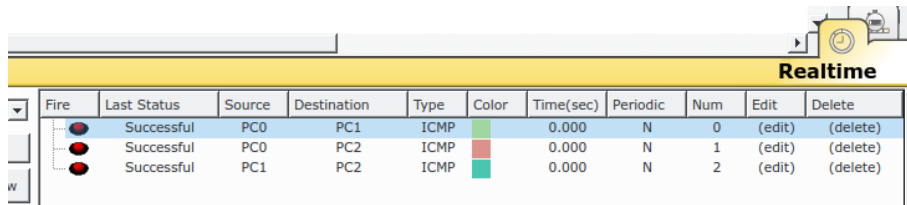
Configuring routers to run RIP is done by the command `'router rip'`, and the specifying which networks to be advertised as being connected to the router, the command to specify connected network is `'network <network ID>'`.

For the previous topology, figure 10, we can negate the effect of the static routing commands by repeating them with `'no'` before each command. Next we configure each of the routers for RIP as follows.

Router	Commands
0	<pre>>router rip >network 10.0.0.0 >network 10.0.4.0</pre>
1	<pre>>router rip >network 10.0.0.0 >network 10.0.1.0 >network 10.0.3.0</pre>
2	<pre>>router rip >network 10.0.1.0 >ip route 10.0.2.0</pre>

Table 3: Commands used to configure RIP in the topology of figure 10.

Testing the configuration we send ping messages between the hosts, shown in figure 12.



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC0	PC1	ICMP		0.000	N	0	(edit)	(delete)
	Successful	PC0	PC2	ICMP		0.000	N	1	(edit)	(delete)
	Successful	PC1	PC2	ICMP		0.000	N	2	(edit)	(delete)

Figure 13: The successful pings between hosts.

3.1.1 IGRP

Similar to RIP, configuring routers to run IGRP is done via the command `'router eigrp <AS number>'`, and the defining the networks connected to each router exactly as done with RIP, one note is that the *autonomous system number* must be the same between to connected routers to advertise to one another. Table shows the configurations of the routers from the topology in figure 10.

Router	Commands
0	<pre>>router eigrp 1 >network 10.0.0.0 >network 10.0.4.0</pre>
1	<pre>>router eigrp 1 >network 10.0.0.0 >network 10.0.1.0 >network 10.0.3.0</pre>
2	<pre>>router eigrp 1 >network 10.0.1.0 >ip route 10.0.2.0</pre>

Table 4: Commands used to configure IGRP in the topology of figure 10.

3.2 OSPF

For the OSPF demonstration let's use the topology shown in figure.

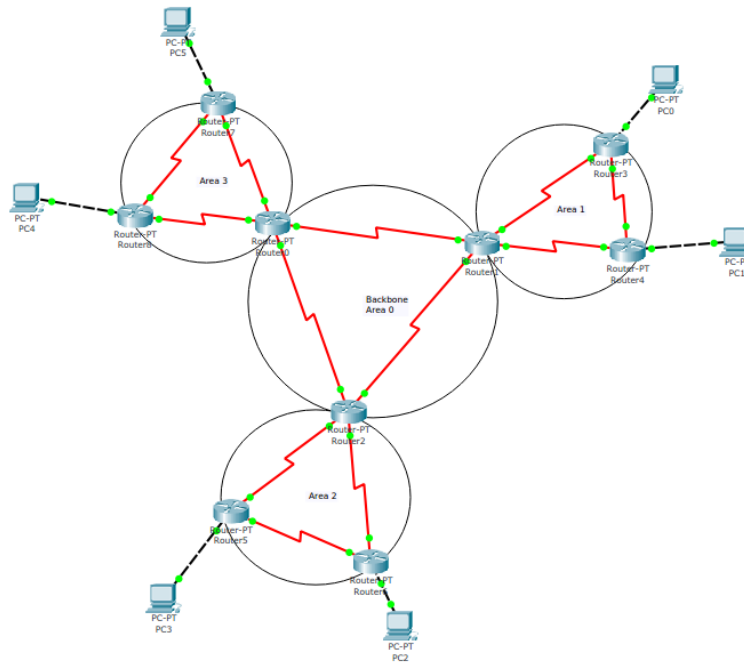


Figure 14: The topology to be used for OSPF. IP's aren't shown here since they over clutter the graph and make it unreadable.

To enable OSPF on routers we use the command `router ospf <process-ID>`, process ID is an arbitrary number recommended to be the same for all routers, though it doesn't affect much. Then, each router must declare which networks it is connected to, and which areas these networks belong to, via the command `network <net-ID> <wildcard-mask> area <area-ID>`, where the wildcard mask is the complement of the subnet mask.

The following table, 5, contains the configuration of the topology made for OSPF.

The following figure 15 shows the successful pings between all hosts in the topology above.

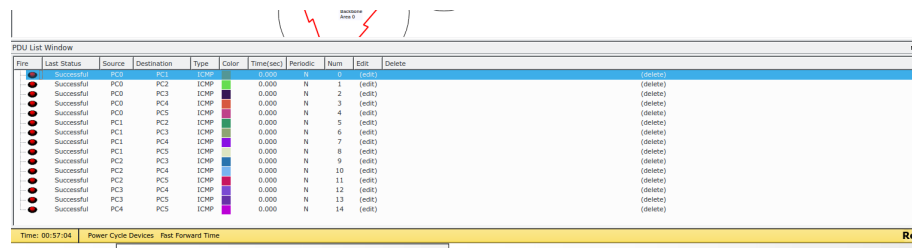


Figure 15: The testing of connectivity between all hosts, achieved by OSPF on the topology of figure 14.

We note that in the commands in table 5 summarization was used, this saved routers 1, 3, 5, 7, and 8 one to two commands each, by implicitly including their information.

Router	Commands
0	<pre>>router ospf 10 >network 193.167.0.0 0.0.0.255 area 0 >network 193.167.2.0 0.0.0.255 area 0 >network 193.170.1.0 0.0.0.255 area 3 >network 193.170.2.0 0.0.0.255 area 3</pre>
1	<pre>>router ospf 10 >network 193.167.0.0 0.0.1.255 area 0 >network 193.168.0.0 0.0.1.255 area 1</pre>
2	<pre>>router ospf 10 >network 193.169.1.0 0.0.0.255 area 2 >network 193.169.2.0 0.0.0.255 area 2 >network 193.167.1.0 0.0.0.255 area 0 >network 193.167.2.0 0.0.0.255 area 0</pre>
3	<pre>>router ospf 10 >network 193.168.2.0 0.0.1.255 area 1 >network 193.168.0.0 0.0.0.255 area 1</pre>
4	<pre>>router ospf 10 >network 193.168.1.0 0.0.0.255 area 1 >network 193.168.2.0 0.0.0.255 area 1 >network 193.168.4.0 0.0.0.255 area 1</pre>
5	<pre>>router ospf 10 >network 193.169.0.0 0.0.1.255 area 2 >network 193.169.4.0 0.0.0.255 area 2</pre>
6	<pre>>router ospf 10 >network 193.169.2.0 0.0.1.255 area 2 >network 193.169.0.0 0.0.0.255 area 2</pre>
7	<pre>>router ospf 10 >network 193.170.0.0 0.0.1.255 area 3 >network 193.170.4.0 0.0.0.255 area 3</pre>
8	<pre>>router ospf 10 >network 193.170.2.0 0.0.1.255 area 3 >network 193.170.0.0 0.0.0.255 area 3</pre>

Table 5: Commands used to configure OSPF in the topology of figure .

Part III

Conclusions

The importance of networks in our everyday lives, has made enterprises in particular pay great attention to their infrastructures. This imposes great challenges on network admins, since they have to be able to create an efficient and robust network to handle all the data flow, and be able to adjust to future expansions, which is not an easy task to do.

Many decisions have to be made in order to create a network, that is sustainable from the get-go. These range from the type of equipment needed, to the types of software to run on said equipment. But one of the most crucial of all these decisions, is how to manage all the data traffic in the network, this is where routing comes in place.

Choosing between static and dynamic routing can be determined mainly based on the network size, for small networks static routing can be very powerful, giving the admin total control to direct the traffic however they may please. But this does have it's toll, which is the tediousness to configure, and flat out impracticality on larger networks, where dynamic routing is preferred.

Deciding on the types of dynamic routing can also be dependant on the network size, medium sized networks can make use of Distance Vector Routing, which doesn't flood the whole network with traffic every now and then to advertise it's info, which is the case for Link State Routing. However, if a network was to be divided into zones, or areas, for security, administrative, or managerial, puposes, then link-state, and more specificaly OSPF, becomes the better choice. This is more evident in the limited number of hops allowed in the two most famous distance vector routing algorithms, RIP and IGRP, which would limit the growth of a large enterprise.

List of Figures

1	An example router schema, showing several interfaces, reference [2].	1
2	Two simplified networks connected via a boundary router. IP#1 belongs to Network 1, while IP#2 belongs to Network 2. IP#1 and IP#2 are connected each to it's own NIC, and are unique to each network it's part of.	2
3	A Cat 5e connection on a laptop, used for Ethernet, reference [4].	2
4	8P8C modular connector, commonly referred to as RJ45, used for the Ethernet standard, reference [4].	3
5	The pin layout of the three types of RJ45 cables.	4
6	Example routing table, using PacketTracer.	4
7	Example of a higherarchical autonomous system, reference [8]. . .	8
8	An example of an summarization scenario.	9
9	IP configuration panel, for the generic PC in PacketTracer. . . .	10
10	Simple topography, distributing IP's. Each device has the IP assign to it's interface, all have subnet mask /24.	12
11	Accessing the configuration mode of Router 1 remotely.	13
12	The success in connecting all hosts using static routin.	15
13	The successful pings between hosts.	16
14	The topology to be used for OSPF. IP's aren't shown here since they over clutter the graph and make it unreadable.	17
15	The testing of connectivity between all hosts, achieved by OSPF on the topology of figure 14.	18

List of Tables

1	Commands used to configure the routers in the topology of figure 10.	14
2	Commands used to configure static routing in the topology of figure 10.	15
3	Commands used to configure RIP in the topology of figure 10. . .	16
4	Commands used to configure IGRP in the topology of figure 10. . .	17
5	Commands used to configure OSPF in the topology of figure . . .	19

References

- [1] Kurose, James and Ross, Keith, 2013. Computer Networking: A Top-Down Approach, 6th edition.
- [2] The lab manuals.
- [3] Treasure of Networking Solutions blog
<http://sorashar.blogspot.com/2012/02/router-interfaces.html>
- [4] Ethernet | Wikipedia
<https://en.wikipedia.org/wiki/Ethernet>
- [5] Routing | Wikipedia
<https://en.wikipedia.org/wiki/Routing>
- [6] RIP | Wikipedia
https://en.wikipedia.org/wiki/Routing_Information_Protocol
- [7] OSPF | Wikipedia
https://en.wikipedia.org/wiki/Open_Shortest_Path_First
- [8] Inter-Area Routing in OSPF | How Unicast IPv4 Routing Protocols and Services Work
https://msdn.microsoft.com/fr-fr/library/cc755330%28v=ws.10%29.aspx#w2k3tr_ucast_how_thyu