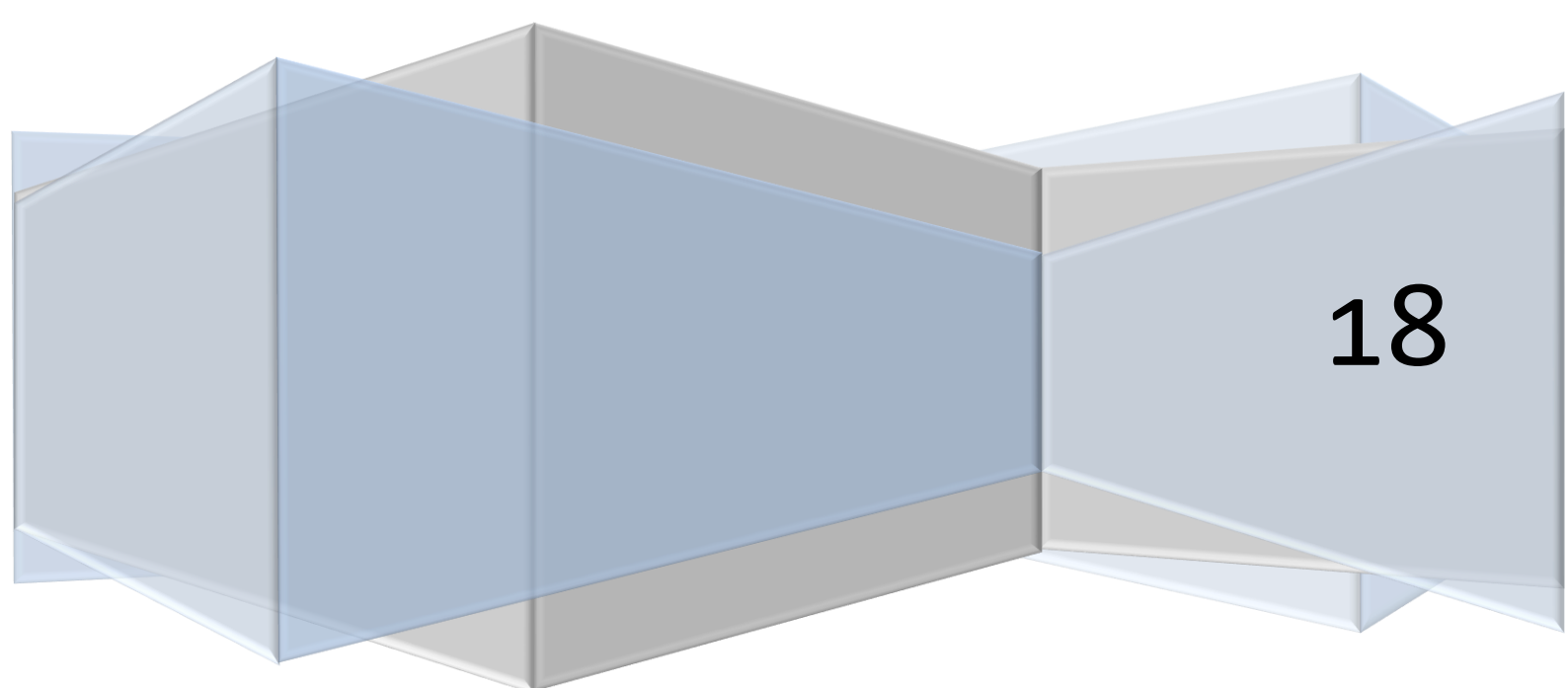


DrayTek Training

Routing in DrayTek Routers (Part 1)

Roy Panetta



18

Table of Contents

1. Course Outline	3
2. IP Basics.....	5
2.1 IP Versions.....	5
2.1.1 IP Version 4 (IPv4)	5
2.1.2 IP Version 6 (IPv6)	8
3. Routing Basics	11
3.1 Routing Protocols.....	12
3.2 Classful vs Classless Routing Protocols	12
3.3 Types of Routing Protocols	13
3.3.1 Routing Information Protocol (RIP).....	13
3.3.2 Interior Gateway Routing Protocol (IGRP)	13
3.3.3 Enhanced Interior Gateway Routing Protocol (EIGRP)	13
3.3.4 Open Shortest Path First (OSPF)	13
3.3.5 Border Gateway Protocol (BGP).....	14
3.4 Routing Decisions.....	15
3.5 Selecting a Routing Protocol	15
3.6 Default Route	16
3.7 Administrative Distance	16
4. The Routing Table	17
4.1 Types of Routes.....	17
4.1.1 Static Route	17
4.1.2 Dynamic Routes	17
4.1.3 Where does the routing information come from?	18
4.2 Configuring Static Routing	19
4.2.1 Configuration Steps.....	19
4.3 Configuring Dynamic Routing	21
4.3.1 Configuration Steps using RIP Protocol	21
5. Inter-LAN Routing.....	23
5.1 Inter-LAN Routing in DrayOS Routers	24
5.2 Inter-LAN Routing in Linux Based Routers	24
5.3 Verifying Settings for Routing	24
6. Hands on Exercises.....	25
6.1 Exercise 1 - Static Routing	25

6.2 Exercise 2 - Dynamic Routing.....	38
---------------------------------------	----

1. Course Outline

- IP Basics
 - IPV4 / IPv6
 - Subnetting
 - Addressing
- What is Routing
 - Routing Overview
 - Routing Protocols
 - The Routing Table
- Types of Routes
 - Static Routing
 - Dynamic Routing
 - Policy-based Routing (Covered in Part 2)
 - Inter-VLAN Routing
 - Verifying Setting for Routing
- Exercises
 - Static Routing
 - Dynamic Routing

(Blank)

2. IP Basics

An Internet Protocol address (IP address) is a numerical label assigned to each device connected to a computer network using Internet Protocol (IP) for communication. Every device in an IP-based network including routers, print servers, and host PCs, needs an IP address to identify the device as well as its location on the network.

In simple terms the function of an IP Address is to allocate a unique address to a device on a network so that any information sent to that device can reach it by referring to its address. It is similar to when you send a letter to your friend. You will have written an address on the envelope, which is analogous to an IP address on a data packet. The letter goes through the postal service and finally is passed onto the postman who searches for the house number written on the address and delivers it to your friend. This is similar to the way IP addresses are used on the data network to deliver data packets to the correct destinations.

2.1 IP Versions

Two versions of the Internet Protocol are in common use in the Internet today, IPv4 and IPv6. IPv4 was first installed in 1983. However, the IPv4 address pool had become exhausted due to the limited address space. This prompted the introduction of IPv6 in 2011 which provides a much greater pool of IP addresses. This will be discussed in more detail in the IPv6 section.

2.1.1 IP Version 4 (IPv4)

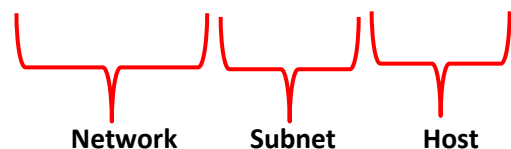
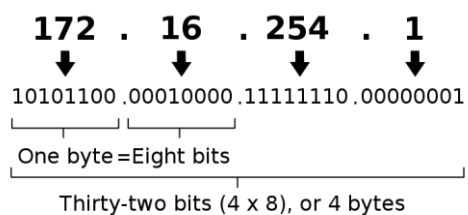
An IP address consists of two parts: the network component and the host component. The Network component can be further broken down into subnets. For example, the IP address shown in the diagram on the right belongs to the 172.16.x.x network and within the network we have the subnet .254. Within each subnet we can have up to 254 devices.

The subnet mask or the Classless Inter-Domain Routing (**CIDR**) prefix determines how the IP address is divided into network and host parts. CIDR is a method for allocating IP addresses and IP routing. The term subnet mask is only used within IPv4.

IP v4 uses 32-bits in its address which limits the address space to 4,294,967,296 (2^{32}) IP addresses.

IP addresses are usually written and displayed in human-readable notation, such as 172.16.254.1

An IPv4 address (dotted-decimal notation)



Subnetting

When the Internet was developed, IP addressing was first designed with no concept of subnets. The classification into A, B, and C networks was done to cater for different size networks to accommodate large, medium and small networks.

Subnetting is used to allow a larger number of individual network assignments. The first three bits of the most significant octet of an IP address is defined as the class of the address. Three classes are defined (A, B, and C) as shown in the table below:

Class	Leading Bits	Number of Networks	Addresses per Network	Start Address	End Address
A	0	128 (2^7)	16,777,216 (2^{24})	0.0.0.0	127.255.255.255
B	10	16,384 (2^{14})	65,536 (2^{16})	128.0.0.0	191.255.255.255
C	110	2,097,152 (2^{21})	256 (2^8)	192.0.0.0	223.255.255.255

Subnet Mask

A Subnet mask is a 32-bit number that masks an IP address, and divides the IP address into network address and host address. Subnet Mask is made by setting network bits to all "1"s and setting host bits to all "0"s. The table below shows the subnet masks for Class A, B and C networks.

Class	Address	# of Hosts	Netmask (Binary)	Netmask (Decimal)
A	/8	16,777,216 (2^{24})	11111111 00000000 00000000 00000000	255.0.0.0
B	/16	65,536 (2^{16})	11111111 11111111 00000000 00000000	255.255.0.0
C	/24	256 (2^8)	11111111 11111111 11111111 00000000	255.255.255.0

Subnet masks can also be used to divide a network into smaller network segments. For example, a /29 subnet mask (255.255.255.248) will give you 8 IP addresses for each network. Applying this to 192.168.1.0 subnet we have the following:

IPv4 address: **192 . 168 . 1 . 0**

Netmask (/29): 11111111 . 11111111 . 11111111. 11111**000**

Number of available addresses = 8 (2^3) 192.168.1.0 to 192.168.1.7

The first IP address is the subnet IP address 192.168.1.0 and the last is the broadcast IP address 192.168.1.7, which are both reserved. This leaves 6 IP addresses which can be assigned to devices.

The table below shows a few of the subnets that can be generated from a class C network using a /29 subnet mask.

Subnet	Mask	Subnet Size	Host Range	Broadcast
192.168.1.0	255.255.255.248	6	192.168.1.1 to 192.168.1.6	192.168.1.7
192.168.1.8	255.255.255.248	6	192.168.1.9 to 192.168.1.14	192.168.1.15
192.168.1.16	255.255.255.248	6	192.168.1.17 to 192.168.1.22	192.168.1.23

Available
addresses = 8 (2^3)

Public IP Addresses

A public IP address is the address that is assigned to a network device to allow it to be directly accessible over the Internet. Devices that may need a public IP addresses are web servers, email servers, routers etc. Each device must be assigned a unique public IP address so that it can be accessed and not conflict with any other device. These public IP addresses are usually allocated by service providers for their customers.

Private IP Addresses

A private IP address is the address space to allow organizations or individual households to create their own private networks. These IP addresses are not used on the public Internet and are usually configured on the router LAN side. The router then uses Network Address Translation (NAT) to translate the private IP addresses of the local network to a public IP address on the router WAN interface.

There are three IP blocks reserved for a private use. These are class A, class B and class C. The table below shows the private IP address ranges that can be used in a private network.

Class	Starting IP Address	Ending IP Address	# of Hosts
A	10.0.0.0	10.255.255.255	16,777,216 (2^{24})
B	172.16.0.0	172.31.255.255	1,048,576 (2^{20})
C	192.168.0.0	192.168.255.255	65,536 (2^{16})

When devices on a local network are assigned a private IP address, the local devices see each other via their private IP address. However, the devices on the Internet cannot directly communicate to the private IP address, but use the router's public IP address to communicate using NAT.

Note: In this document the term **hosts** refer to any network attached devices such as servers, PCs, workstations, laptops, routers, IP phones, Access Points etc.

2.1.2 IP Version 6 (IPv6)

IPv6 Development

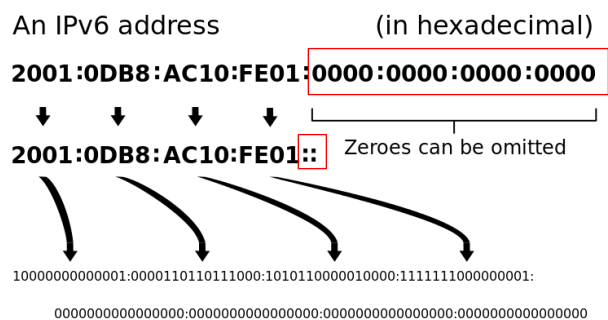
Internet Protocol IPv4 was first developed in the 1970s and at the time it was thought to be more than enough to handle all the network devices in the world. However, since it uses 32 bits for addressing, this limited the number of possible IP addresses. With the expansion of the internet it became apparent that the original assumptions were not correct and this resulted in a shortage in the number of available IPv4 addresses. This was mainly due to the explosion in the number and range of IP capable devices that are continuously being released in the market.

An interim method is to use NAT in routers so that a single public IP address can be shared by a large number of devices behind the router. To overcome this, IPv6 was developed to increase the number of available IP addresses. Since IPv6 uses 128 bits for its address, it allows an almost unlimited number of IP addresses that can be used. So now it will be possible for every device to be connected to the internet and to also have a unique IP address.

IPv6 Addressing

IPv6 uses 128-bits or 16 octets (16 x 8 bits) in its address. This provides an address space of 2^{128} (approximately 3.403×10^{38} IP addresses) which is significantly larger than the IPv4 address space which uses 32-bits in its address.

Successive quartets of 0's can be omitted and replaced with :: as shown in the example here.



IPv6 Private Addresses

IPv6 private IP addresses do exist. However, these cannot be routed to the public network.

IPv6 private addressing is called Unique Local Addresses (ULA). In the IPv4 world, private addresses include 10.0.0.0-10.255.255.255, and 172.16.0.0-172.31.255.255, and 192.168.0.0-192.168.255.255. In the IPv6 world, the ULA space is fc00::/7, or basically anything that starts with FD in the IPv6 address, so fdxx:xxxx:xxxx...

Note: The /7 notation refers to the subnet mask. So /7 means 7 1's followed by 121 0's, meaning that the first seven bits in the IP address do not change.

IPv6 Public Addresses

IPv6 public addressing is called Global Unicast (GU). It works like public IPv4 addresses which include

1.0.0.0 - 9.255.255.255
11.0.0.0 - 126.255.255.255
129.0.0.0 - 169.253.255.255
169.255.0.0 - 172.15.255.255
172.32.0.0 - 191.0.1.255
192.0.3.0 - 192.88.98.255
192.88.100.0 - 192.167.255.255
192.169.0.0 - 198.17.255.255
198.20.0.0 - 223.255.255.255

The GU usually has many prefixes but originally it starts with 2 or 3. e.g 2xxx:xxxx:xxxx...

IPv6 Link-Local Addresses

IPv6 link-local addresses works like an IPv4 APIPA (Automatic Private IP Addressing) from Microsoft Windows. These addresses cannot be routed, it is allocated automatically when a device has not been configured with a static IP address and cannot find a DHCP. This includes 169.254.0.0-169.254.254.254. For IPv6 link local addresses, it starts with a prefix of FE80:xxxx:xxxx...

Guidelines in shortening IPv6 address

1. Leading zeroes in a quartet are optional. For example, the quartet 08A5 equals 8A5 and the quartet 0000 equals 0.
2. Successive quartets of zeros can be represented as two colons "::". But this method can only be use once in an address. For example, 3120:0:F130:0000:0000:C90:6A78:13B0 can be written as 3120:0:F130::C90:6A78:13B0.

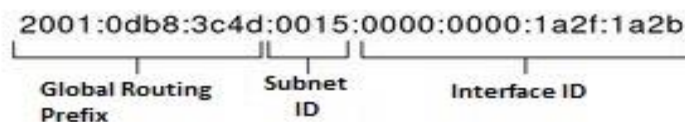
Guidelines in expanding an IPv6 address.

1. In each quartet, add leading 0s as needed until the quartet has 4 hex digits.
2. If double colon (::) exists, count all the quartets, replace (::) with multiple quartets of 0000 so that the total is 8 quartets.

Parts of IPv6 Address

- Global Routing Prefix is the first three groupings of numbers (first 48 bits). It is also called Network ID used for routing.
- Subnet ID is the fourth grouping of numbers (the 49th through 64th bits). It is the number that identifies the subnet within a site. Functions like the subnet field of IPv4 addresses.
- Interface ID is the last four groupings of numbers (the last 64 bits). Which act like an IPv4 host field.

Example:



Network Ranges for Prefix Lengths of IPv6

The prefix-length specifies a range of devices. It is expressed as a slash (/), followed by an integer between 1 through 128. For example, a prefix-length of /64 specified like this:

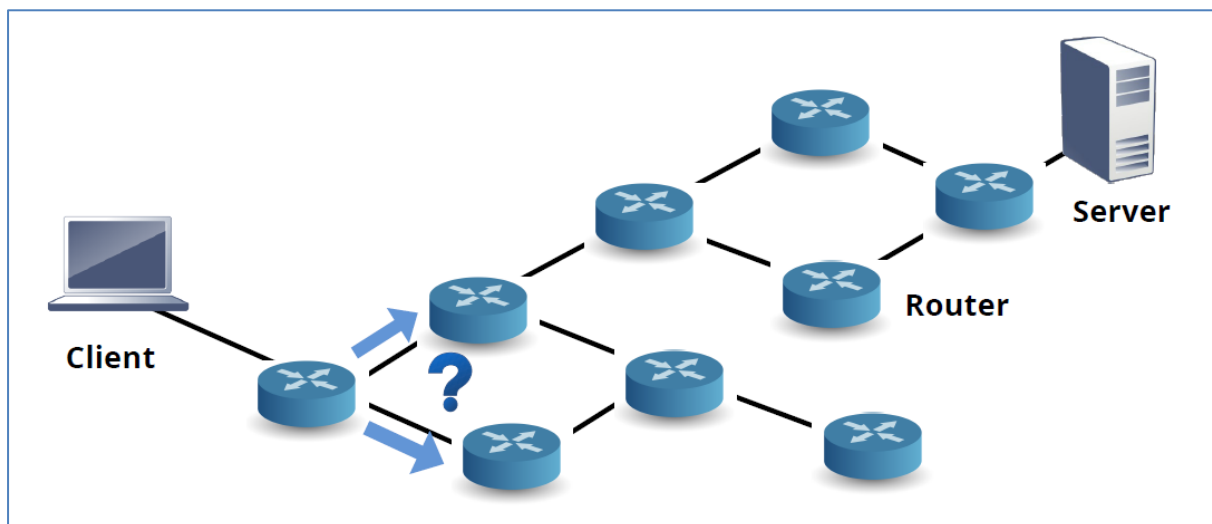
`2001:db8:abcd:0012::/64` tells the system to divide the network into 64 subnetworks. Each subnetwork contains 1/64th of the devices on the network.

Expanded Notation	Abbreviation Notation	Prefix Length	Device Range in Subnetwork
<code>2001:0DB8:ABCD:0012:0000:0000:0000:0000</code>	<code>2001:DB8:ABCD:12::</code>	<code>2001:DB8:ABCD:12::0/64</code>	<code>2001:0DB8:ABCD:0012:0000:0000:0000:0000 - 2001:0DB8:ABCD:0012:FFFF:FFFF:FFFF:FFFF</code>

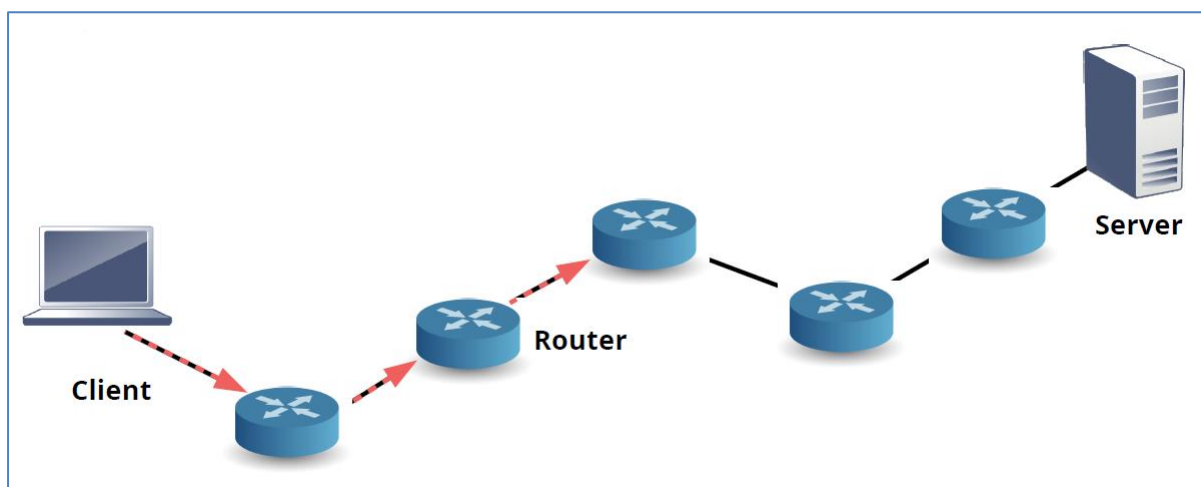
3. Routing Basics

An analogy to routing is the postal service which takes your mail and routes it to its destination. Routers use a routing protocol to route data (selecting a path for traffic) in a network, between or across multiple networks. Routing protocols accomplish this task by maintaining routing tables. Routers usually have two or more interfaces to connect to different networks, so the information in the routing tables are used as it contains a list of networks and how to reach them.

For example, in a large network, each router maintains a routing table that is used to select the correct path for the data. In the diagram below, the server is only reachable through a certain router. When the client PC sends out a data packet, each router's routing protocol will look up the destination network in its routing table. If the destination network is the same as the source network, the routing protocol drops and ignores the data packet. Otherwise, it routes the data out of the appropriate router interface to the destination network or another attached router that is connected or closer to the destination network.



Each router selects the best path for packets according to their destination



Routers selected the best path from Client to the Server

3.1 Routing Protocols

Routing protocols specify how routers communicate with each other, disseminating information that enables them to select routes between any two nodes on a network. Routing algorithms are used to work out the best choice for each route. Each router has prior knowledge of only networks attached to it directly.

3.2 Classful vs Classless Routing Protocols

Classful routing protocols do not send subnet mask information with their routing updates. This means that the attached routers need to use a common subnet mask otherwise the router will use a subnet mask corresponding to the IP subnet class, i.e. class A, B or C also known as “major network”

Belonging to same “major network” simply indicates that they belong to the same “classful” network. For example:

- 10.3.1.0 and 10.5.5.0 belong to the same major network (10.0.0.0)
- 10.1.4.5 and 11.1.4.4 do not belong to the same major network
- 192.168.1.1 and 192.168.1.254 belong to the same major network (192.168.1.0)
- 192.168.1.5 and 192.167.2.5 do not belong to the same major network.

Classless routing protocols do send the subnet mask with their updates. Thus, Variable Length Subnet Masks (VLSMs) are allowed when using classless routing protocols.

Examples of classful routing protocols are RIPv1 and IGRP.

Examples of classless routing protocols are RIPv2, EIGRP, OSPF, and IS-IS.

3.3 Types of Routing Protocols

Three major classes are in use for routing protocols. These are:

- **Interior gateway protocols type 1**, link-state routing protocols, such as OSPF and IS-IS
- **Interior gateway protocols type 2**, distance-vector routing protocols, such as Routing Information Protocol, RIPv2, IGRP.
- **Exterior gateway protocols** are routing protocols used on the Internet for exchanging routing information between Autonomous Systems, such as Border Gateway Protocol (BGP), Path Vector Routing Protocol.

Definition: An Autonomous System is a connected group of one or more Internet Protocol prefixes run by one or more network operators which has a SINGLE and CLEARLY DEFINED routing policy.

3.3.1 Routing Information Protocol (RIP)

This is a distance-vector routing protocol employing hop count as a routing metric. RIP prevents routing loops by implementing a limit on the number of hops allowed in a path from source to destination. The maximum number of hops allowed for RIP is 15. Two versions of RIP are available:

- **RIP Version 1** - The original specification of RIP which uses classful routing. The periodic routing updates do not carry subnet information, so subnet masks are fixed according to the “major network” as described in section 3.2. This limitation makes it impossible to have different-sized subnets inside of the same network class. This means that all subnets must use the same subnet mask.
- **RIP Version 2** – In addition to RIP v1, it includes the ability to carry subnet information, thus supporting Classless Inter-Domain Routing (CIDR). To maintain backward compatibility, the hop count limit of 15 remains.

3.3.2 Interior Gateway Routing Protocol (IGRP)

This is a proprietary protocol developed by Cisco to overcome the limitations of RIP. It is a distance vector interior gateway protocol (IGP) used by routers to exchange routing data within an autonomous system.

3.3.3 Enhanced Interior Gateway Routing Protocol (EIGRP)

This is a proprietary protocol developed by Cisco. It is an advanced distance-vector routing protocol that is used on a computer network for automating routing decisions and configuration.

3.3.4 Open Shortest Path First (OSPF)

This is a routing protocol for Internet Protocol (IP) networks. It uses a link state routing (LSR) algorithm and falls into the group of interior gateway protocols (IGPs), operating within a single autonomous system (AS).

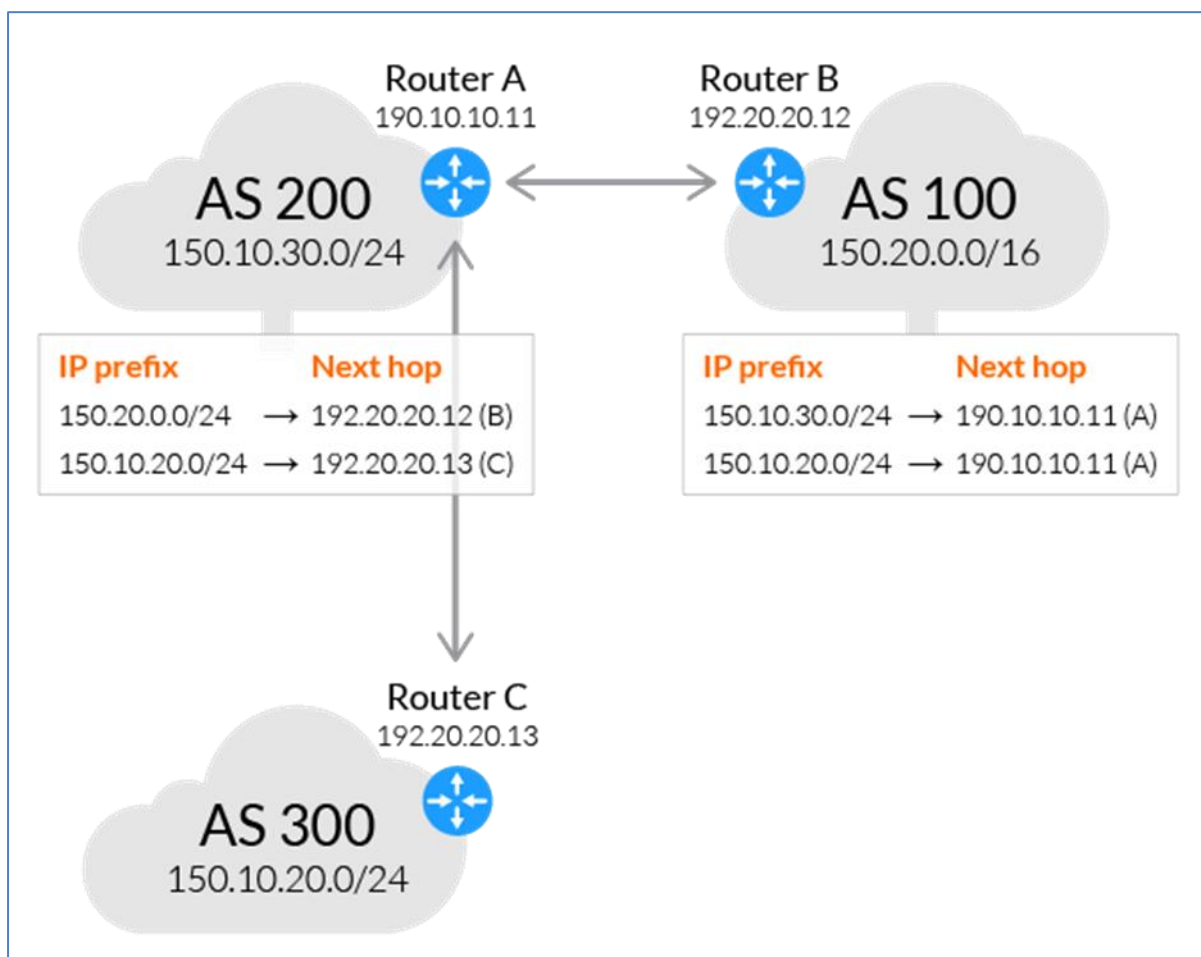
3.3.5 Border Gateway Protocol (BGP) - A definition from Wikipedia is *“it is a standardized exterior gateway protocol designed to exchange routing and reachability information among autonomous systems (AS) on the Internet. The protocol is often classified as a path vector protocol but is sometimes also classed as a distance-vector routing protocol.”*

An **Autonomous System (AS)** can be an Internet Service Provider, a university or an entire corporate network, including multiple locations (IP addresses). Each **AS** is represented by a unique number called an ASN.

In this type of network architecture, each autonomous system controls a collection of connected routing prefixes, representing a range of IP addresses.

Each autonomous system will have a “peer” which exchanges routing information with its neighbouring peers in the form of network prefix announcements. This information is used to dynamically calculate the best data path to a destination network.

In the diagram below, we have three autonomous systems: AS 100, AS 200 and AS 300. BGP exchanges routing information between each of these autonomous systems

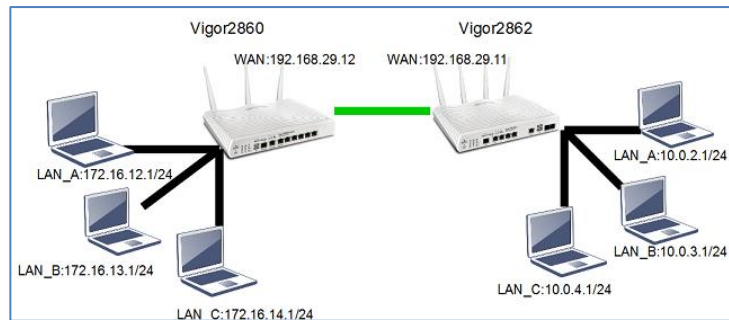


DrayTek routers supporting BGP are: Vigor3900, Vigor2960, Vigor300B, Vigor2860, Vigor2862, Vigor2926, Vigor2952 and Vigor3220 running the latest firmware.

DrayTek has an application note showing how to configure BGP between a Vigor2862 and a Vigor2860.

More details in the following URL:

<https://www.draytek.com/en/faq/faq-connectivity/connectivity.lbpr/how-to-establish-bgp-connection/>



3.4 Routing Decisions

When more than one route is available to a destination network, a router needs to determine which path to take. This decision is accomplished by using metrics (*cost values used by routers to determine the best path to a destination network*). The type of metric used is based on the routing protocol used as shown in the table below.

Definition: A **metric** is a variable used in a router to work out which path to take in forwarding data packets. Router metrics can contain any number of values that help the router determine the best route among multiple routes to a destination.

Routing Protocol	Metric
RIP Version 1 and RIP Version 2	Hops
IGRP	Bandwidth, delay, reliability, load and MTU
EIGRP	Bandwidth, delay, reliability, load and MTU
OSPF	Bandwidth
BGP	Weight, local preference, multi-exit discriminator

Routing metrics are assigned to each router link to determine which route to a destination will be the shortest. The route with the lowest metric will be deemed to be the shortest path to a destination.

3.5 Selecting a Routing Protocol

The choice of routing protocol will depend on what is supported in the router as well as complexity of the network. For small networks within an organisation that are not directly connected to the Internet, the network administrator decides which routing protocol to use. For larger networks directly connected to the internet such as those run by Internet Service Providers (ISP), the routing protocol to use is usually determined by the network that they are connected to.

For simple networks, static routing may be sufficient. For an internetwork with fewer than 16 hops with links having equal bandwidth, RIP protocol will be a suitable solution. However, for an Internetwork with fewer than 16 hops but with links of unequal bandwidth, the use of IGRP, EIGRP or OSPF will be more suitable as these protocols will take the bandwidth of each link into consideration.

3.6 Default Route

The routing table is used by a router to send data from a network device to a destination host or network. For destination networks not in the routing table, a default route is configured in the router. This will send all data packets for unknown destination networks to the interface corresponding to the default route setting.

In the example below, all packets destined for unknown networks are sent to WAN 1 (168.95.98.254).

Current Running Routing Table		IPv6 Routing Table	
Key: C - connected, S - static, R - RIP, * - default, ~ - private			
*	0.0.0.0/ 0.0.0.0	via 168.95.98.254	WAN1
S	42.69.245.219/ 255.255.255.255	via 42.69.245.219	USB1

You will notice that all zeros are used for the destination/subnet mask (0.0.0.0/0.0.0.0). The zeros indicate unknown values. If a specific route was added to the routing table, the zeros will be replaced with a valid IP address and subnet mask. For example, a specific route is in the next entry in the routing table above (42.69.245.219/255.255.255.255).

3.7 Administrative Distance

On large internetworks, multiple routing protocols are often used. For example, there could be a mixture of Static Routes, RIP and OSPF routing protocols being used. So, the question arises of which route the router will use to transport the data. A solution is to look at the Administrative Distance for a particular route. The Administrative Distance is a number from 0 to 255 and indicates the reliability of the route's source. The lower the administrative distance, the more reliable the source so will be the preferred route for the data packet.

The table below shows the default administrative distance for each type of routing protocol.

Routing Protocol	Administrative Distance
Directly connected interface	0
Static route	1
EIGRP summary route	5
External BGP	20
Internal EIGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
EGP	140
External EIGRP	170
Internal BGP	200
Unknown Source	255

4. The Routing Table

Each Router maintains a routing table, which is list of preferred routes to different networks.

The routing table below is from a Vigor2860 router. The first column shows type of route:

C	Connected	(The WAN interface is directly connected to this IP address)
S	Static	(Route entry is manually entered in “LAN >> Static Route Setup” menu)
R	RIP	(Route learned using RIP routing protocol)
*	Default route	(Default path if no other routes exist to a destination)
~	Private	

There are 3 parts, being the Destination IP /Subnet Mask, Gateway and Interface.

Diagnostics >> View Routing Table

Current Running Routing Table		IPv6 Routing Table	
Key: C - connected, S - static, R - RIP, * - default, ~ - private			
*	0.0.0.0/ 0.0.0.0	via 168.95.98.254	WAN1
S	42.69.245.219/ 255.255.255.255	via 42.69.245.219	USB1
*	100.103.34.49/ 255.255.255.255	via 100.103.34.49	USB2
C	100.103.34.48/ 255.255.255.252	directly connected	USB2
C~	192.168.1.0/ 255.255.255.0	directly connected	LAN1
S	111.251.233.158/ 255.255.255.255	via 111.251.233.158	WAN1
*	168.95.98.254/ 255.255.255.255	via 168.95.98.254	WAN1
Destination IP + Subnet Mask		Gateway	Interface

4.1 Types of Routes

There are two ways a router learns a route: static and dynamic. A good overview describing the differences between static routes and dynamic routes is covered in the following YouTube video available from the Professor Messer YouTube Channel:

What is the difference between a static route and a dynamic route?”

<https://youtu.be/HA4YZWrqzxU>

4.1.1 Static Route

These routes are manually configured in the router to specify routes to other networks. Static routing is suitable for small networks. These entries appear in the routing table with the key “S” shown on the first column. This method however is unfeasible for larger networks where topologies can change rapidly.

4.1.2 Dynamic Routes

Dynamic routes are routes that a router learns by using a routing protocol and are more common on the Internet. The router learns the routes from neighbouring routers running the same routing protocols. As described in section 3.3 examples of dynamic-routing protocols and algorithms include Routing Information Protocol (**RIP**), Open Shortest Path First (**OSPF**) and Enhanced Interior Gateway Routing Protocol (**EIGRP**)

4.1.3 Where does the routing information come from?

Routing information is derived from sources listed below:

- Direct connection (WAN & LAN)
- VPN connection
- Static Routing
- Dynamic Routing

The routing table below shows some different types of routes.

Diagnostics >> View Routing Table

Current Running Routing Table		IPv6 Routing Table	
Key: C - connected, S - static, R - RIP, * - default, ~ - private			
*	0.0.0.0/ 0.0.0.0	via 168.95.98.254	WAN1
C~	192.168.11.0/ 255.255.255.0	directly connected	LAN1
C~	192.168.12.0/ 255.255.255.0	directly connected	LAN2
C~	192.168.13.0/ 255.255.255.0	directly connected	LAN3
C~	192.168.14.0/ 255.255.255.0	directly connected	LAN4
S~	192.168.1.0/ 255.255.255.0	via 111.248.122.210	VPN-1
S	111.251.169.163/ 255.255.255.255	via 111.251.169.163	WAN1

4.2 Configuring Static Routing

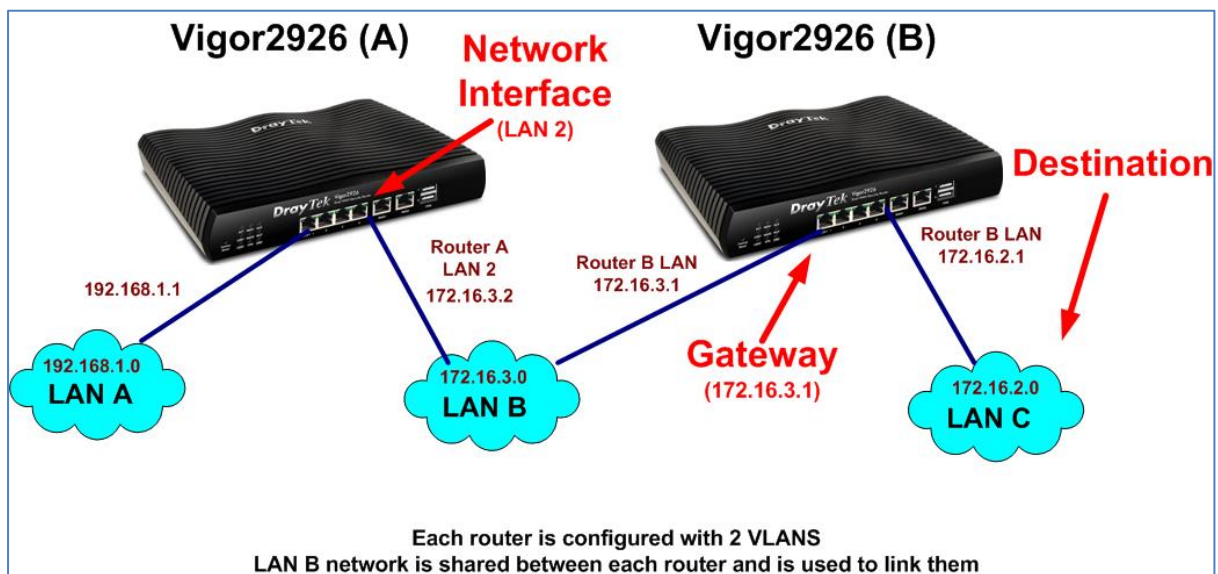
In the diagram below a static route is used to allow a device on LAN A to be able to communicate with a device on LAN C. Each router has two networks and LAN B is a common network shared between the two routers to link them together.

Vigor2926 (A) router has two networks

- **LAN A** – 192.168.1.0 directly connected to router LAN 1
- **LAN B** – 172.16.3.0 directly connected to router LAN 2

Vigor2926 (B) router has two networks

- **LAN B** – 172.16.3.0 directly connected to router LAN 1
- **LAN C** – 172.16.2.0 directly connected to router LAN 2



4.2.1 Configuration Steps

In the Vigor2926 (A) Router, go to **LAN >>Static Route** configuration menu.

- Click on an available index
- Enter the details as shown below:
- Click **OK** to save the settings

LAN >> Static Route Setup

Index No. 1

☒ Enable

Destination IP Address	172.16.2.0
Subnet Mask	255.255.255.0
Gateway IP Address	172.16.3.1
Network Interface	LAN2 ▼

OK Cancel Delete

- Go to **Diagnostics>>View Routing Table**

The routing table will show the static route as highlighted below.

Diagnostics >> View Routing Table			
IPv4			
Key	Destination	Gateway	Interface
C~	192.168.1.0/ 255.255.255.0	directly connected	LAN1
S~	172.16.2.0/ 255.255.255.0	via 172.16.3.1	LAN2
C~	172.16.3.0/ 255.255.255.0	directly connected	LAN2

Vigor2926 (B) Static Route Setting

Routing >> Static Route Setup	
Index No. 1	
☒ Enable	
Destination IP Address	192.168.1.0
Subnet Mask	255.255.255.0
Gateway IP Address	172.16.3.2
Network Interface	LAN1 ▼
OK	Cancel Delete

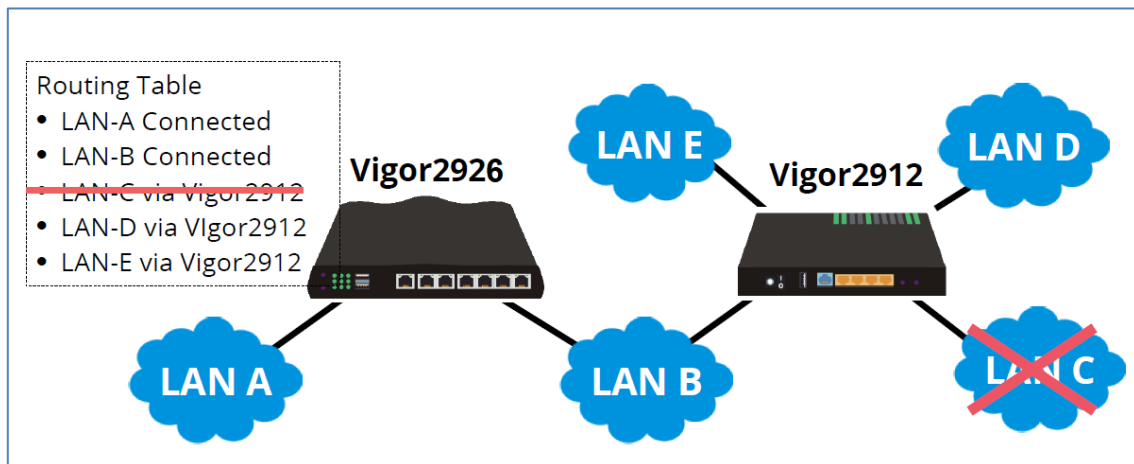
Vigor2926 (B) Routing Table

Diagnostics >> View Routing Table			
IPv4			
Key	Destination	Gateway	Interface
S~	192.168.1.0/ 255.255.255.0	via 172.16.3.2	LAN1
C~	172.16.2.0/ 255.255.255.0	directly connected	LAN2
C~	172.16.3.0/ 255.255.255.0	directly connected	LAN1

This shows that Vigor2926 (A) Router knows that to get to subnet 172.16.2.0 it needs to send the data to LAN 2 which has the IP address of 172.16.3.1. The second router Vigor2926 (B) knows that subnet 172.16.2.0 is directly connected to its LAN 2. Therefore, data from a PC on LAN A can find its way to a device on LAN C through the configured static routes.

4.3 Configuring Dynamic Routing

Dynamic routing allows the router to select a data path according to real-time logical network changes. This information is derived from information exchanged between routers, such as availability of networks. For example, if a network goes down, the routing tables will be automatically updated with the routing changes. In the diagram below when LAN C goes down the route to LAN C will be removed from the routing table.



Dynamic Routing requires a supported routing protocol. Routing protocols supported in DrayTek routers are:

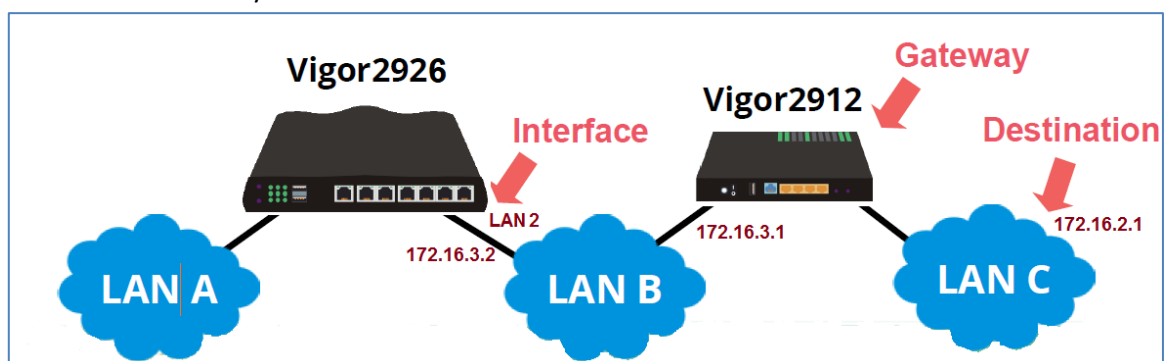
- **RIPv2** (Routing Information Protocol) - *DrayOS and Linux Models*
- **OSPF** (Open Shortest Path First) - *Linux models only*
- **BGP** (Border Gateway Protocol) - *Linux models & Vigor2860/2862/2926/2952/3220 running latest firmware*
(More details on BGP is available in section 3.3.5 in this manual)
- **IS-IS** (not supported)
- **EIGRP** (not supported)

4.3.1 Configuration Steps using RIP Protocol

We will use the example below and enable RIP Protocol so that the route can be discovered and the routing table can be updated. Then a PC connected to LAN A can connect to a device on LAN C.

Existing entries in the Vigor2926 routing are:

- **LAN A** - directly connected – LAN 1
- **LAN B** - directly connected - LAN 2



WAN Connections

In the router go to **WAN >> Internet Access** menu and enable RIP protocol as shown in the diagram below:

WAN >> Internet Access

WAN 1

PPPoE **Static or Dynamic IP** PPTP/L2TP IPv6

☒ Enable ☐ Disable

Keep WAN Connection

☐ Enable PING to keep alive

PING to the IP:

PING Interval: 0 minute(s)

WAN Connection Detection

Mode: ARP Detect

MTU

1500 (Max: 1500)

Path MTU Discovery: Detect

RIP Protocol

☒ Enable RIP

Bridge Mode

☐ Enable Bridge Mode

Bridge Subnet: LAN 1

WAN IP Network Settings **WAN IP Alias**

☒ Obtain an IP address automatically

Router Name:

Domain Name:

☐ DHCP Client Identifier *

Username:

Password:

☐ Specify an IP address

IP Address:

Subnet Mask:

Gateway IP Address:

☒ Default MAC Address

☐ Specify a MAC Address

MAC Address: 00 1D AA 56 39 21

DNS Server IP Address:

LAN Connections

In the router, go to **LAN >> General Setup** configuration menu for each LAN and enable **RIP Protocol Control**.

LAN >> General Setup

LAN 1 Ethernet TCP / IP and DHCP Setup **LAN 1 IPv6 Setup**

Network Configuration

For NAT Usage

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

RIP Protocol Control: Enable

DHCP Server Configuration

☒ Enable Server ☐ Disable Server

☐ Enable Relay Agent

Start IP Address: 192.168.1.10

IP Pool Counts: 200

Gateway IP Address: 192.168.1.1

Lease Time: 86400 (s)

☒ Clear DHCP lease for inactive clients periodically

DNS Server IP Address

Primary IP Address:

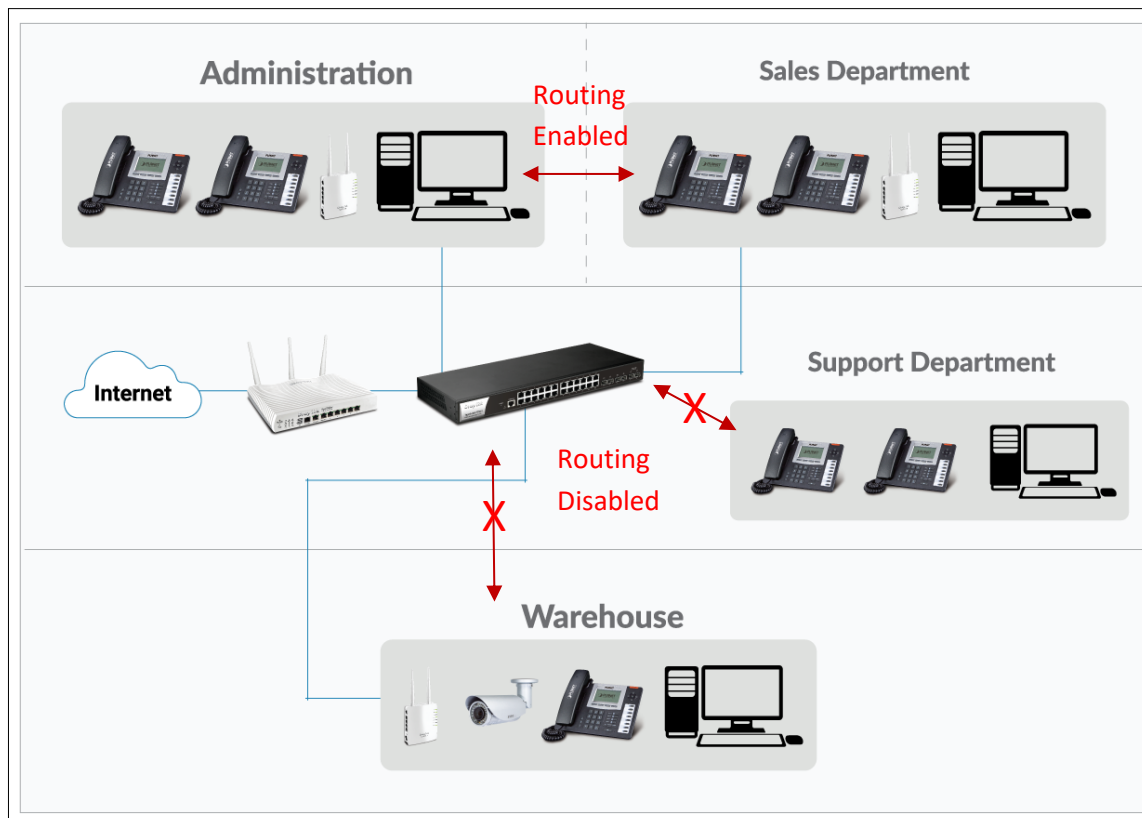
Secondary IP Address:

Note: Change IP Address or Subnet Mask in Network Configuration will also change HA LAN1 Virtual IP to the same domain IP.

OK

5. Inter-LAN Routing

Inter-LAN routing allows communication between different LANS on the network. As shown in the example in the diagram below, you may want to allow the Administration staff to be able to access data or services in the Sales Department. To do this we enable inter-LAN routing between these two LANS. Other departments such as the support department and the warehouse are not allowed access to the sales or administration networks, so we do not allow Inter-LAN routing here.



5.1 Inter-LAN Routing in DrayOS Routers

Traffic between VLANs (or LAN subnets) needs to be routed by the router. Routing across VLANs is allowed only when inter-LAN routing is enabled.

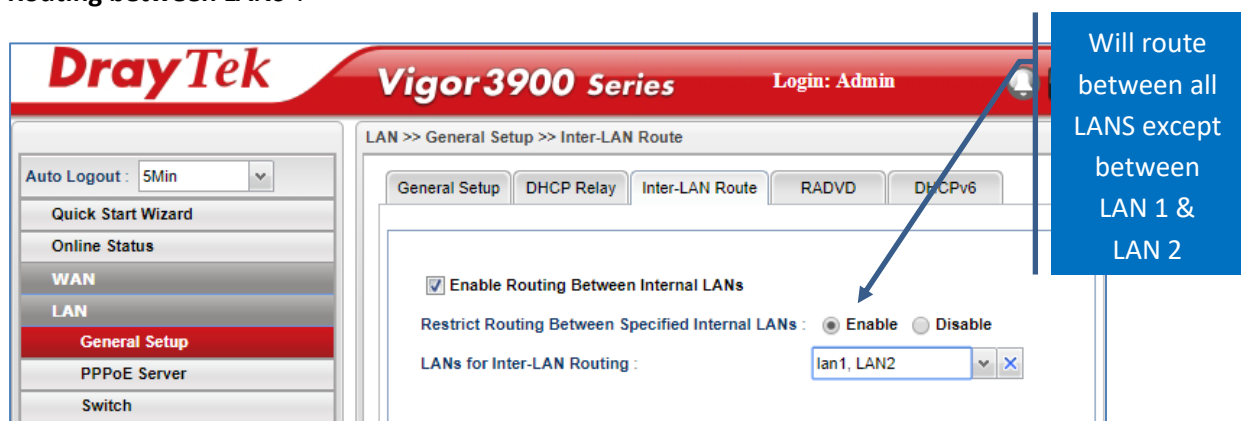
To enable routing between LAN subnets in DrayOS routers, go **LAN >> General Setup** and in the **Inter-LAN Routing** section select the intersection of the LANs that need to be routed in the matrix. In the example below, we enable routing between LAN 1 and LAN 2.

Inter-LAN Routing					
Subnet	LAN 1	LAN 2	LAN 3	LAN 4	LAN 5
LAN 1	☒	☐	☐	☐	☐
LAN 2	☒	☒	☐	☐	☐
LAN 3	☐	☐	☒	☐	☐
LAN 4	☐	☐	☐	☒	☐
LAN 5	☐	☐	☐	☐	☒

5.2 Inter-LAN Routing in Linux Based Routers

Linux based routers such as the Vigor3900, Vigor2960 and Vigor300B have a different menu option for Inter-LAN Routing. The latest firmware 1.3.2 and above now allows you to select which LAN subnets to route.

To enable Inter-LAN routing, go to "**LAN>>General Setup>>Inter-LAN Route**" and select "**Enable Routing between LANs**".



5.3 Verifying Settings for Routing

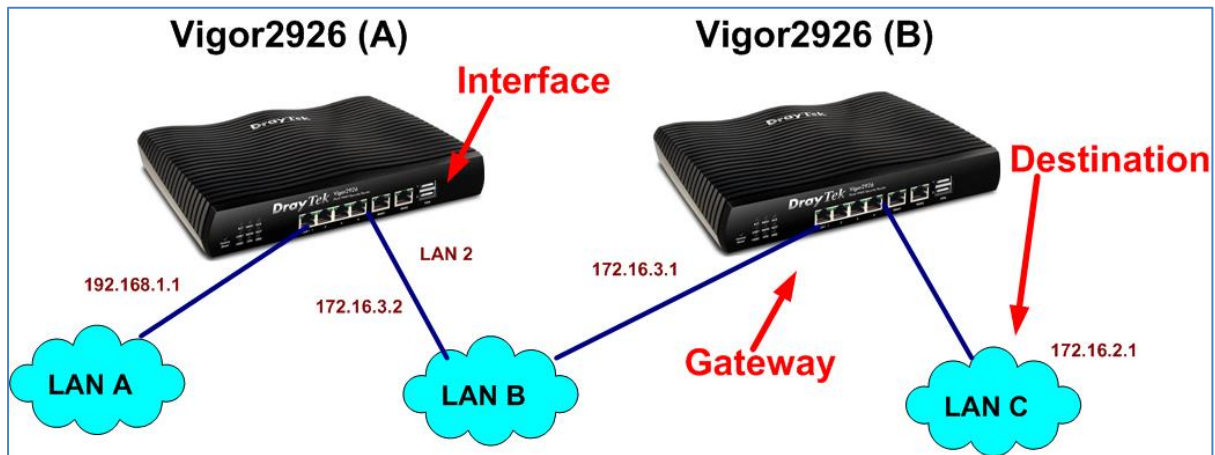
Use "Trace Route" command to test if data packets are forwarded to the correct route.

```
Tracing route to www.draytek.com [104.25.32.24]
over a maximum of 30 hops:
  0  <1 ms    <1 ms    <1 ms    172.16.3.1
  1  17 ms     16 ms     17 ms     h254.s98.ts.hinet.net [168.95.98.254]
  2  19 ms     19 ms     18 ms     sczs-3302.hinet.net [168.95.25.218]
  3  18 ms     17 ms     23 ms     220-128-8-254.HINET-IP.hinet.net [220.128.8.254]
  4  20 ms     20 ms     20 ms     TPD1-3012.hinet.net [220.128.2.150]
  5  18 ms     18 ms     18 ms     r4102-s2.tp.hinet.net [220.128.7.69]
  6  22 ms     20 ms     19 ms     r4002-s2.tp.hinet.net [220.128.11.141]
  7  149 ms    156 ms    146 ms     r12-la.us.hinet.net [211.72.108.17]
  8  149 ms    147 ms    146 ms     202-39-84-74.HINET-IP.hinet.net [202.39.84.74]
  9  161 ms    187 ms    168 ms     xe0-1-0.losangeles2.loa.seabone.net [89.221.35.149]
 10  251 ms    250 ms    148 ms     cloudflare.losangeles2.loa.seabone.net [89.221.35.189]
 11  153 ms    153 ms    153 ms     104.25.32.24
Trace complete.
```

6. Hands on Exercises

6.1 Exercise 1 - Static Routing

Configure static routing between two Vigor2926 routers as shown in the diagram below:



The IP addresses shown in the diagram above are for each LAN in the routers.

Each router has two VLANs and in this exercise, we will set up routing so that devices on LAN A (192.168.1.0 subnet) can communicate with devices on LAN C (172.16.2.0 subnet).

Step 1:

1.1 Configure two VLANs in Vigor2926 (A)

- Log into the router using the IP address 192.168.1.1 (*username/password admin/admin*).
- Go to **LAN>>VLAN Configuration** menu.
- Select **Enable**.
- Select **P1** and **P2** to be members of **VLAN0** and subnet **LAN 1**.
- Select **P3** and **P4** to be members of **VLAN1** and subnet **LAN 2**.
- Click **OK** to save the settings. (*The router will restart to save the settings*)

LAN >> VLAN Configuration

VLAN Configuration

☒ Enable

	LAN				Subnet	VLAN Tag		
	P1	P2	P3	P4		Enable	VID	Priority
VLAN0	☒	☒	☐	☐	LAN 1 ▼	☐	0	0 ▼
VLAN1	☐	☐	☒	☒	LAN 2 ▼	☐	0	0 ▼
VLAN2	☐	☐	☐	☐	LAN 1 ▼	☐	0	0 ▼
VLAN3	☐	☐	☐	☐	LAN 1 ▼	☐	0	0 ▼
VLAN4	☐	☐	☐	☐	LAN 1 ▼	☐	0	0 ▼
VLAN5	☐	☐	☐	☐	LAN 1 ▼	☐	0	0 ▼
VLAN6	☐	☐	☐	☐	LAN 1 ▼	☐	0	0 ▼
VLAN7	☐	☐	☐	☐	LAN 1 ▼	☐	0	0 ▼
VLAN8	☐	☐	☐	☐	LAN 1 ▼	☐	0	0 ▼
VLAN9	☐	☐	☐	☐	LAN 1 ▼	☐	0	0 ▼
VLAN10	☐	☐	☐	☐	LAN 1 ▼	☐	0	0 ▼
VLAN11	☐	☐	☐	☐	LAN 1 ▼	☐	0	0 ▼
VLAN12	☐	☐	☐	☐	LAN 1 ▼	☐	0	0 ▼
VLAN13	☐	☐	☐	☐	LAN 1 ▼	☐	0	0 ▼
VLAN14	☐	☐	☐	☐	LAN 1 ▼	☐	0	0 ▼
VLAN15	☐	☐	☐	☐	LAN 1 ▼	☐	0	0 ▼

☒ Permit untagged device in P1 to access router

1.2 Configure LAN Subnets in Vigor2926 (A)

1.2.1 Configure LAN A

- Go to **LAN>>General Setup** Configuration menu.
- Click on **Details Page** button for LAN 1.

LAN >> General Setup

General Setup

Index	Status	DHCP	IP Address		
LAN 1	V	V	192.168.1.1	Details Page	IPv6
LAN 2	☒	☒	172.16.3.2	Details Page	IPv6

- For LAN 1 check that you have the settings as shown below. These should be the default settings.

LAN >> General Setup

LAN 1 Ethernet TCP / IP and DHCP Setup

Network Configuration
For NAT Usage

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

RIP Protocol Control: Disable ▼

LAN 1 IPv6 Setup

DHCP Server Configuration

☐ Disable ☒ Enable Server ☐ Enable Relay Agent

Start IP Address: 192.168.1.10

IP Pool Counts: 200 (max. 1021)

Gateway IP Address: 192.168.1.1

Lease Time: 86400 (s)

☒ Clear DHCP lease for inactive clients periodically

DNS Server IP Address

Primary IP Address:

Secondary IP Address:

Note: Change IP Address or Subnet Mask in Network Configuration will also change HA LAN1 Virtual IP to the same domain IP.

1.2.2 Configure LAN B

- Go to **LAN>>General Setup** Configuration menu.
- Click on **Details Page** button for LAN 2.
- Select **Enable**.
- Select **"For NAT Usage"** option.
- Enter the LAN IP address 172.16.3.2
- Enter DHCP settings as shown below.
 - *Enable Server*
 - *Start IP Address:* 172.16.3.10
 - *IP Pool Counts:* 100
 - *Gateway IP Address:* 172.16.3.2
- Click **OK** to save settings (*The router will restart to save the settings*).

LAN >> General Setup

LAN 2 Ethernet TCP / IP and DHCP Setup

Network Configuration

☒ Enable ☐ Disable

☒ For NAT Usage ☐ For Routing Usage

IP Address

Subnet Mask

LAN 2 IPv6 Setup

DHCP Server Configuration

☐ Disable ☒ Enable Server ☐ Enable Relay Agent

Start IP Address

IP Pool Counts (max. 1021)

Gateway IP Address

Lease Time (s)

☒ Clear DHCP lease for inactive clients periodically.

DNS Server IP Address

Primary IP Address

Secondary IP Address

Note: Change IP Address or Subnet Mask in Network Configuration will also change HA LAN2 Virtual IP to the same domain IP.

1.2.3 Enable Inter-LAN Routing

- Go to **LAN>>General Setup** Configuration menu.
- Select the intersection of LAN 1 and LAN 2 as shown in the diagram below.
- Click **OK** to save settings

Inter-LAN Routing

Subnet	LAN 1	LAN 2	LAN 3	LAN 4	LAN 5	LAN 6	LAN 7	LAN 8	DMZ Port
LAN 1	☒	☐	☐	☐	☐	☐	☐	☐	☐
LAN 2	☒	☒	☐	☐	☐	☐	☐	☐	☐
LAN 3	☐	☐	☒	☐	☐	☐	☐	☐	☐
LAN 4	☐	☐	☐	☒	☐	☐	☐	☐	☐
LAN 5	☐	☐	☐	☐	☒	☐	☐	☐	☐
LAN 6	☐	☐	☐	☐	☐	☒	☐	☐	☐
LAN 7	☐	☐	☐	☐	☐	☐	☒	☐	☐
LAN 8	☐	☐	☐	☐	☐	☐	☐	☒	☐
DMZ Port	☐	☐	☐	☐	☐	☐	☐	☐	☒

Note:
LAN2/3/4/5/6/7/8 are available when VLAN is enabled.

Step 2:

2.1 Configure two VLANs in Vigor2926 (B)

- Log into the router using the IP address 192.168.1.1 (*username/password admin/admin*).
- Go to **LAN>>VLAN Configuration** menu.
- Select **Enable**.
- Select **P1** and **P2** to be members of **VLAN0** and subnet **LAN 1**.
- Select **P3** and **P4** to be members of **VLAN1** and subnet **LAN 2**.
- Click **OK** to save the settings. (*The router will restart to save the settings*)

LAN >> VLAN Configuration

VLAN Configuration

☒ Enable

	LAN				Subnet	VLAN Tag		
	P1	P2	P3	P4		Enable	VID	Priority
VLAN0	☒	☒	☐	☐	LAN 1 ▼	☐	0	0 ▼
VLAN1	☐	☐	☒	☒	LAN 2 ▼	☐	0	0 ▼
VLAN2	☐	☐	☐	☐	LAN 1 ▼	☐	0	0 ▼
VLAN3	☐	☐	☐	☐	LAN 1 ▼	☐	0	0 ▼
VLAN4	☐	☐	☐	☐	LAN 1 ▼	☐	0	0 ▼
VLAN5	☐	☐	☐	☐	LAN 1 ▼	☐	0	0 ▼
VLAN6	☐	☐	☐	☐	LAN 1 ▼	☐	0	0 ▼
VLAN7	☐	☐	☐	☐	LAN 1 ▼	☐	0	0 ▼
VLAN8	☐	☐	☐	☐	LAN 1 ▼	☐	0	0 ▼
VLAN9	☐	☐	☐	☐	LAN 1 ▼	☐	0	0 ▼
VLAN10	☐	☐	☐	☐	LAN 1 ▼	☐	0	0 ▼
VLAN11	☐	☐	☐	☐	LAN 1 ▼	☐	0	0 ▼
VLAN12	☐	☐	☐	☐	LAN 1 ▼	☐	0	0 ▼
VLAN13	☐	☐	☐	☐	LAN 1 ▼	☐	0	0 ▼
VLAN14	☐	☐	☐	☐	LAN 1 ▼	☐	0	0 ▼
VLAN15	☐	☐	☐	☐	LAN 1 ▼	☐	0	0 ▼

☒ Permit untagged device in P1 to access router

2.2 Configure LAN Subnets in Vigor2926 (B)

2.2.1 Configure LAN A

- Go to **LAN>>General Setup** Configuration menu.
- Click on **Details Page** button for LAN 1.

LAN >> General Setup

General Setup

Index	Status	DHCP	IP Address	Details Page	IPv6
LAN 1	V	V	192.168.1.1	Details Page	IPv6
LAN 2	☒	☒	192.168.2.1	Details Page	IPv6

- Enter the LAN IP address 172.16.3.1
- Enter DHCP settings as shown below:
 - *Enable Server*
 - *Start IP Address:* 172.16.3.100
 - *IP Pool Counts:* 155 (Can leave at default value)
 - *Gateway IP Address:* 172.16.3.1
- Click **OK** to save settings (*The router may reboot to save and activate the new settings*).

Vigor2926 Series

LAN >> General Setup

LAN 1 Ethernet TCP / IP and DHCP Setup	LAN 1 IPv6 Setup
Network Configuration For NAT Usage IP Address: 172.16.3.1 Subnet Mask: 255.255.255.0 RIP Protocol Control: Disable ▼	DHCP Server Configuration ☐ Disable ☒ Enable Server ☐ Enable Relay Agent Start IP Address: 172.16.3.100 IP Pool Counts: 155 (max. 1021) Gateway IP Address: 172.16.3.1 Lease Time: 86400 (s) ☒ Clear DHCP lease for inactive clients periodically DNS Server IP Address Primary IP Address: Secondary IP Address:

Note: Change IP Address or Subnet Mask in Network Configuration will also change HA LAN1 Virtual IP to the same domain IP.

2.2.2 Configure LAN B

- Go to **LAN>>General Setup** Configuration menu.
- Click on **Details Page** button for LAN 2.

LAN >> General Setup

General Setup

Index	Status	DHCP	IP Address		
LAN 1	V	V	172.16.3.1	Details Page	IPv6
LAN 2	☒	☒	192.168.2.1	Details Page	IPv6

- Enter the LAN IP address 172.16.2.1
- Enter DHCP settings as shown below:
 - *Enable Server*
 - *Select "For NAT Usage" option.*
 - *Start IP Address: 172.16.2.10*
 - *IP Pool Counts: 100*
 - *Gateway IP Address: 172.16.2.1*
- Click **OK** to save settings (*The router may reboot to save and activate the new settings*).

Vigor2926 Series

LAN >> General Setup

LAN 2 Ethernet TCP / IP and DHCP Setup

Network Configuration

☒ Enable ☐ Disable

☒ For NAT Usage ☐ For Routing Usage

IP Address: 172.16.2.1

Subnet Mask: 255.255.255.0

LAN 2 IPv6 Setup

DHCP Server Configuration

☐ Disable ☒ Enable Server ☐ Enable Relay Agent

Start IP Address: 172.16.2.10

IP Pool Counts: 100 (max. 1021)

Gateway IP Address: 172.16.2.1

Lease Time: 259200 (s)

☒ Clear DHCP lease for inactive clients periodically.

DNS Server IP Address

Primary IP Address:

Secondary IP Address:

Note: Change IP Address or Subnet Mask in Network Configuration will also change HA LAN2 Virtual IP to the same domain IP.

2.2.3 Enable Inter-LAN Routing

- Go to **LAN>>General Setup** Configuration menu.
- Select the intersection of LAN 1 and LAN 2 as shown in the diagram below.

Inter-LAN Routing

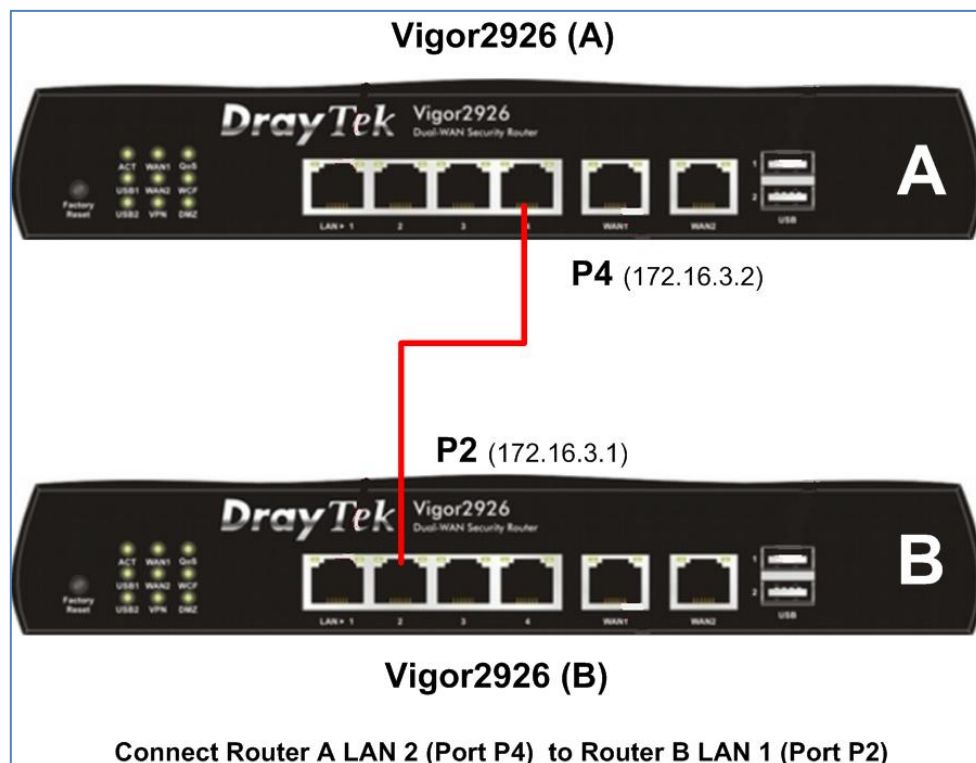
Subnet	LAN 1	LAN 2	LAN 3	LAN 4	LAN 5	LAN 6	LAN 7	LAN 8	DMZ Port
LAN 1	☒	☐	☐	☐	☐	☐	☐	☐	☐
LAN 2	☒	☒	☐	☐	☐	☐	☐	☐	☐
LAN 3	☐	☐	☒	☐	☐	☐	☐	☐	☐
LAN 4	☐	☐	☐	☒	☐	☐	☐	☐	☐
LAN 5	☐	☐	☐	☐	☒	☐	☐	☐	☐
LAN 6	☐	☐	☐	☐	☐	☒	☐	☐	☐
LAN 7	☐	☐	☐	☐	☐	☐	☒	☐	☐
LAN 8	☐	☐	☐	☐	☐	☐	☐	☒	☐
DMZ Port	☐	☐	☐	☐	☐	☐	☐	☐	☒

Note:
LAN2/3/4/5/6/7/8 are available when VLAN is enabled.

OK

Step 3: Connect Router A to Router B

Connect the two routers as shown below: Use a short Ethernet cable and connect LAN port P4 on router A to LAN port P2 on router B. This will link the two routers over a common subnet (172.16.3.0)



Step 4: Testing

Check Routing Table in Each Router

- Connect your laptop to LAN port 1 on Vigor2926 A router, connect to 192.168.1.1
- For the second router (Vigor2926 B) connect the laptop to LAN port 1, connect to 172.16.3.1
- On each router, go to **Diagnostics >> Routing Table** page and check the current routing table.

You should see the directly connected routes on the local router but not the routes from the other router.

Router A

Vigor2926 Series

Diagnostics >> View Routing Table

IPv4 | [Refresh](#) |

Key	Destination	Gateway	Interface
C~	192.168.1.0/ 255.255.255.0	directly connected	LAN1
C~	172.16.3.0/ 255.255.255.0	directly connected	LAN2

Key
C: Connected S: Static R: RIP *: default ~: private B: BGP

Router B

Vigor2926 Series

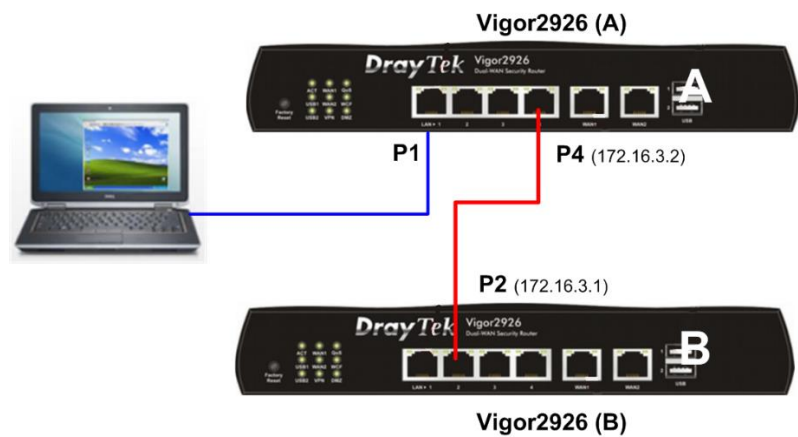
Diagnostics >> View Routing Table

IPv4

Key	Destination	Gateway	Interface
C~	172.16.2.0/ 255.255.255.0	directly connected	LAN2
C~	172.16.3.0/ 255.255.255.0	directly connected	LAN1

4.1 Testing with no Static Routes Enabled

Connect your PC to
router A LAN port 1.



Test using Router Diagnostic Feature

- Go to **Diagnostics >> Ping Diagnosis** menu in the router and try to ping each of the following IP addresses:

192.168.1.1 172.16.3.2 172.16.3.1 172.16.2.1	
---	--

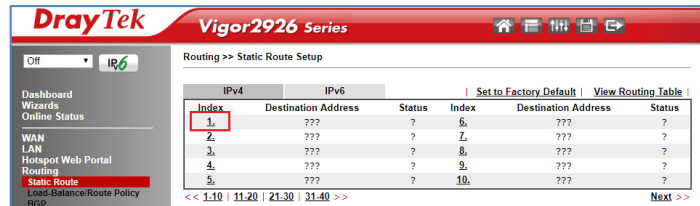
You should be able to ping 192.168.1.1, 172.16.3.1 and 172.16.3.2 but get no response from 172.16.2.1. This is due to no routes enabled to 172.16.2.0 subnet.

You can also test ping from the PC command prompt and see similar results.

Step 5: Enable Static Routes in Each Router

5.1 Configure Static Route in Vigor2926 (A)

- Log into the router using the IP address 192.168.1.1 (*username/password admin/admin*).
- Go to **Routing >> Static Route Setup** Configuration menu.
- Select Index 1
- Select **Enable**.
- Enter the destination IP address 172.16.2.0
- Enter subnet mask: 255.255.255.0
- Enter Gateway IP address 172.16.3.1
- Select network interface: LAN2
- Click OK to save



Routing >> Static Route Setup

Index No. 1

☒ Enable

Destination IP Address: 172.16.2.0

Subnet Mask: 255.255.255.0

Gateway IP Address: 172.16.3.1

Network Interface: LAN2

OK Cancel Delete

5.2 Configure Static Route in Vigor2926 (B)

- Log into the router B using the IP address 172.16.3.1 (*username/password admin/admin*).
- Go to **Routing >> Static Route Setup** Configuration menu.
- Select Index 1
- Select **Enable**.
- Enter the destination IP address 192.168.1.0
- Enter subnet mask: 255.255.255.0
- Enter Gateway IP address 172.16.3.2
- Select network interface: LAN1
- Click **OK** to save

Routing >> Static Route Setup

Index No. 1

☒ Enable

Destination IP Address: 192.168.1.0

Subnet Mask: 255.255.255.0

Gateway IP Address: 172.16.3.2

Network Interface: LAN1

OK Cancel Delete

Step 6: Check Routing Table in Each Router

On each router, go to **Diagnostics >> Routing Table** page and check the current routing table.

You should see the directly connected routes on the local as well as the static routes just configured.

Router A

Diagnostics >> View Routing Table				
IPv4				
Key	Destination	Gateway	Interface	
C~	192.168.1.0/ 255.255.255.0	directly connected	LAN1	
S~	172.16.2.0/ 255.255.255.0	via 172.16.3.1	LAN2	
C~	172.16.3.0/ 255.255.255.0	directly connected	LAN2	

Router B

Diagnostics >> View Routing Table				
IPv4				
Key	Destination	Gateway	Interface	
S~	192.168.1.0/ 255.255.255.0	via 172.16.3.2	LAN1	
C~	172.16.2.0/ 255.255.255.0	directly connected	LAN2	
C~	172.16.3.0/ 255.255.255.0	directly connected	LAN1	

Step 7. Testing with Static Routes Enabled

Test from Router A

Connect your PC to router A LAN port 1 and try to ping each of the following IP addresses:

192.168.1.1
172.16.3.2
172.16.3.1
172.16.2.1

You should be able to ping all the IP addresses and be able to connect to 172.16.2.1 with your web browser.

```
C:\Users\Roy Panetta>ping 172.16.2.1

Pinging 172.16.2.1 with 32 bytes of data:
Reply from 172.16.2.1: bytes=32 time<1ms TTL=254
Reply from 172.16.2.1: bytes=32 time<1ms TTL=254
Reply from 172.16.2.1: bytes=32 time<1ms TTL=254
Reply from 172.16.2.1: bytes=32 time<1ms TTL=254

Ping statistics for 172.16.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Test from Router B

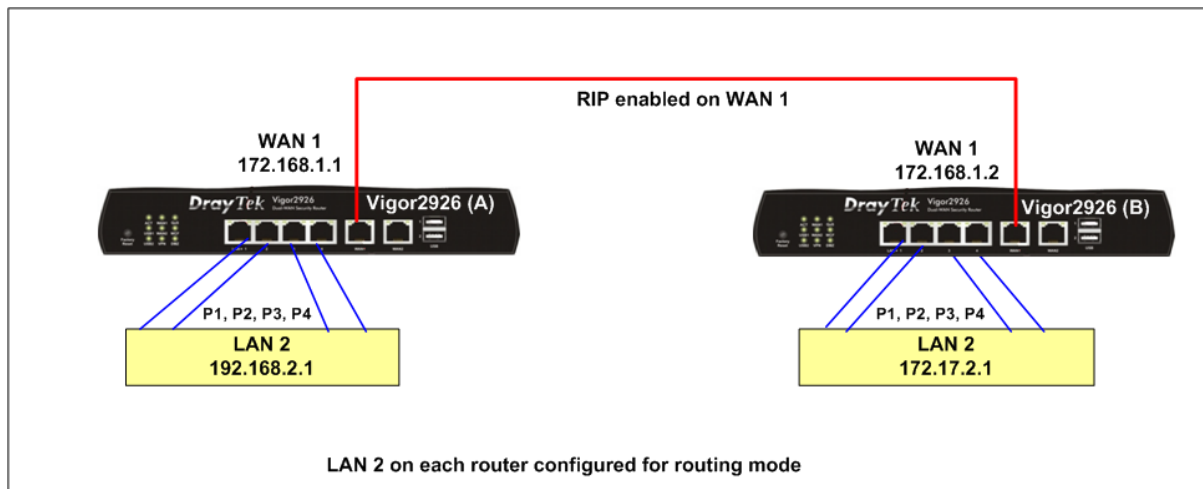
Connect your PC to router B LAN port 1 and try to ping each of the following IP addresses:

192.168.1.1
172.16.3.2
172.16.3.1
172.16.2.1

You should be able to ping all the IP addresses and be able to connect to 192.168.1.1 with your web browser.

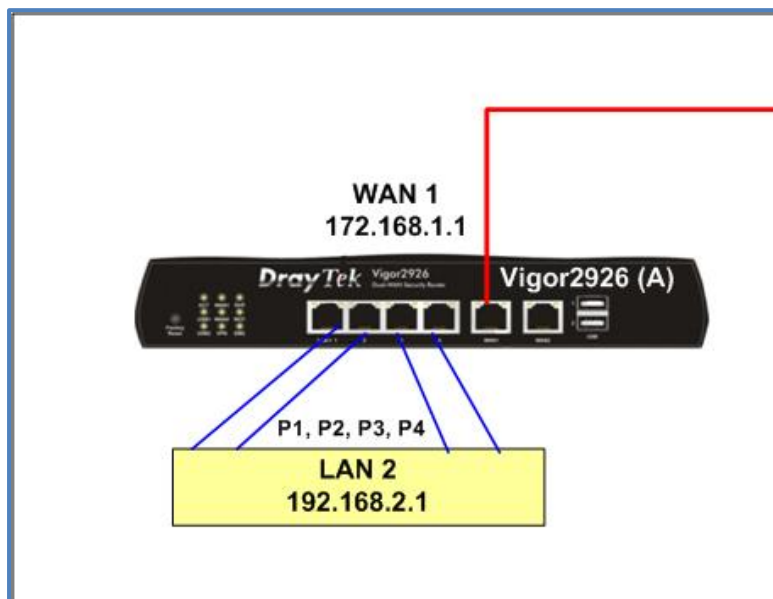
6.2 Exercise 2 - Dynamic Routing

In this exercise we will configure dynamic routing using RIP protocol between two Vigor2926 routers as shown in the diagram below:



Note: The routers will need to be re-configured for this exercise.
Reset each router to factory default configuration before starting the exercise.

Step 1: Configure Router A



1.1 Configure VLAN in Vigor2926 (A)

- (Connect your PC to Router LAN Port 1)
- Log into the Vigor2926 (A) router using the IP address 192.168.1.1 (*username/password admin/admin*).
- Go to **LAN>>VLAN Configuration** menu.
- Select **Enable**.
- Select **P1, P2, P3 and P4** to be members of **VLAN1** and subnet **LAN 2**.
- Click **OK** to save the settings.

Vigor2926 Series

LAN >> VLAN Configuration

VLAN Configuration

☒ Enable

	LAN				Subnet	VLAN Tag		
	P1	P2	P3	P4		Enable	VID	Priority
VLAN0	☐	☐	☐	☐	LAN 1 ▼	☐	0	0 ▼
VLAN1	☒	☒	☒	☒	LAN 2 ▼	☐	0	0 ▼
VLAN2	☐	☐	☐	☐	LAN 1 ▼	☐	0	0 ▼
VLAN3	☐	☐	☐	☐	LAN 1 ▼	☐	0	0 ▼
VLAN4	☐	☐	☐	☐	LAN 1 ▼	☐	0	0 ▼
VLAN5	☐	☐	☐	☐	LAN 1 ▼	☐	0	0 ▼
VLAN6	☐	☐	☐	☐	LAN 1 ▼	☐	0	0 ▼
VLAN7	☐	☐	☐	☐	LAN 1 ▼	☐	0	0 ▼
VLAN8	☐	☐	☐	☐	LAN 1 ▼	☐	0	0 ▼
VLAN9	☐	☐	☐	☐	LAN 1 ▼	☐	0	0 ▼
VLAN10	☐	☐	☐	☐	LAN 1 ▼	☐	0	0 ▼
VLAN11	☐	☐	☐	☐	LAN 1 ▼	☐	0	0 ▼
VLAN12	☐	☐	☐	☐	LAN 1 ▼	☐	0	0 ▼
VLAN13	☐	☐	☐	☐	LAN 1 ▼	☐	0	0 ▼
VLAN14	☐	☐	☐	☐	LAN 1 ▼	☐	0	0 ▼
VLAN15	☐	☐	☐	☐	LAN 1 ▼	☐	0	0 ▼

☒ Permit untagged device in P1 to access router

Note:

- For each VLAN row, selecting Enable VLAN Tag will apply the associated VID to the selected wired LAN port.
- Each VID must be unique.

OK

Clear

Cancel

1.2: Configure LAN Subnet in Vigor2926 (A)

1.2.1 Configure LAN 2

- Go to **LAN>>General Setup** Configuration menu.
- Click on **Details Page** button for LAN 2.

LAN >> General Setup

General Setup

Index	Status	DHCP	IP Address		
LAN 1	V	V	192.168.1.1	Details Page	IPv6
LAN 2	☒	☒	192.168.2.1	Details Page	IPv6
LAN 3	☐	☒	192.168.3.1	Details Page	IPv6

- Configure LAN 2 to use 192.168.2.1 and enable DHCP server as shown below.
- Select “**For Routing Usage**” option.
- Click **OK** to save the setting. *(The router may restart to save and activate the settings)*

LAN >> General Setup

LAN 2 Ethernet TCP / IP and DHCP Setup

LAN 2 IPv6 Setup

Network Configuration

☒ Enable ☐ Disable

☐ For NAT Usage ☒ **For Routing Usage**

IP Address: 192.168.2.1

Subnet Mask: 255.255.255.0

DHCP Server Configuration

☐ Disable ☒ Enable Server ☐ Enable Relay Agent

Start IP Address: 192.168.2.10

IP Pool Counts: 100 (max. 1021)

Gateway IP Address: 192.168.2.1

Lease Time: 259200 (s)

☒ Clear DHCP lease for inactive clients periodically.

DNS Server IP Address

Primary IP Address:

Secondary IP Address:

Note: Change IP Address or Subnet Mask in Network Configuration will also change **HA** LAN2 Virtual IP to the same domain IP.

OK

Once completed, the LAN settings should appear as shown below:

LAN >> General Setup

General Setup

Index	Status	DHCP	IP Address		
LAN 1	V	V	192.168.1.1	Details Page	IPv6
LAN 2	☒	☒	192.168.2.1	Details Page	IPv6
LAN 3	☐	☒	192.168.3.1	Details Page	IPv6

Step 2: Configure WAN 1 – Router A

- Log into the router using the IP address 192.168.2.1
- Go to **WAN >> Internet Access** menu
- Select **Static or Dynamic IP** for WAN 1
- Click on **Details Page** button for WAN 1

WAN >> Internet Access

Internet Access

Index	Display Name	Physical Mode	Access Mode		
WAN1		Ethernet	Static or Dynamic IP	Details Page	IPv6
WAN2		Ethernet	Static or Dynamic IP	Details Page	IPv6
WAN3		USB	None	Details Page	IPv6
WAN4		USB	None	Details Page	IPv6

Note:

- Select **Enable**.
- Select **Enable RIP** for “RIP Protocol” setting.
- Select Specify an IP address.
- Enter IP address 172.168.1.1, Netmask: 255.255.255.0, Gateway 172.168.1.2
- Click **OK** to save.

WAN >> Internet Access

WAN 1

☒ Enable
 ☐ Disable

Keep WAN Connection

☐ Enable PING to keep alive
 PING to the IP
 PING Interval minute(s)

WAN Connection Detection

Mode

MTU

Path MTU Discovery (Max:1500)
 Path MTU Discovery

RIP Protocol

☒ Enable RIP

Bridge Mode

☐ Enable Bridge Mode
 Bridge Subnet

BPA Setup (For Australia Only)

☐ BPA Enable
 Login Server

WAN IP Network Settings

☐ Obtain an IP address automatically
 Router Name
 Domain Name
☐ DHCP Client Identifier
 Username
 Password

☒ Specify an IP address
 IP Address
 Subnet Mask
 Gateway IP Address

☒ Default MAC Address
☐ Specify a MAC Address
 MAC Address:

DNS Server IP Address

Primary IP Address
 Secondary IP Address

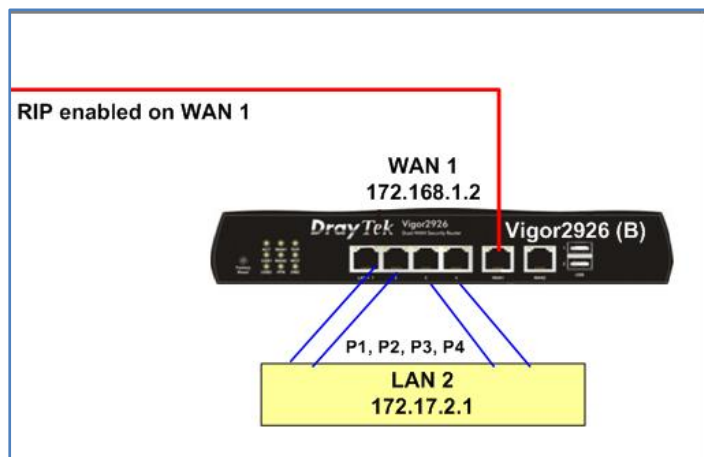
Step 3: Enable Remote Management in Router A

- Log into the router using the IP address 192.168.2.1
- Go to **System Maintenance >> Management** menu in the router.
- Enter the settings as shown below:
 - Select **Allow management from the Internet**
 - Select **HTTP Server**
 - Deselect **Disable PING from the Internet**
 - Click **OK** to save (*Router will restart to save the settings*)

System Maintenance >> Management

IPv4 Management Setup	IPv6 Management Setup	LAN Access Setup																																	
Router Name DrayTek																																			
☐ Default: Disable Auto-Logout ☐ Enable Validation Code in Internet/LAN Access																																			
Internet Access Control ☒ Allow management from the Internet Domain name allowed ☐ FTP Server ☒ HTTP Server ☐ Enforce HTTPS Access ☒ HTTPS Server ☐ Telnet Server ☐ TR069 Server ☐ SSH Server ☐ SNMP Server ☐ Disable PING from the Internet																																			
Access List from the Internet <table border="1"> <thead> <tr> <th>List</th> <th>index in IP Object</th> <th>IP / Mask</th> </tr> </thead> <tbody> <tr><td>1</td><td> </td><td> </td></tr> <tr><td>2</td><td> </td><td> </td></tr> <tr><td>3</td><td> </td><td> </td></tr> <tr><td>4</td><td> </td><td> </td></tr> <tr><td>5</td><td> </td><td> </td></tr> <tr><td>6</td><td> </td><td> </td></tr> <tr><td>7</td><td> </td><td> </td></tr> <tr><td>8</td><td> </td><td> </td></tr> <tr><td>9</td><td> </td><td> </td></tr> <tr><td>10</td><td> </td><td> </td></tr> </tbody> </table>			List	index in IP Object	IP / Mask	1			2			3			4			5			6			7			8			9			10		
List	index in IP Object	IP / Mask																																	
1																																			
2																																			
3																																			
4																																			
5																																			
6																																			
7																																			
8																																			
9																																			
10																																			
Management Port Setup ☒ User Define Ports ☐ Default Ports Telnet Port 23 (Default: 23) HTTP Port 80 (Default: 80) HTTPS Port 443 (Default: 443) FTP Port 21 (Default: 21) TR069 Port 8069 (Default: 8069) SSH Port 22 (Default: 22)																																			
Brute Force Protection ☐ Enable brute force login protection ☐ FTP Server ☐ HTTP Server ☐ HTTPS Server ☐ Telnet Server ☐ TR069 Server ☐ SSH Server Maximum login failures 0 times Penalty period 0 seconds																																			
Blocked IP List																																			
TLS/SSL Encryption Setup ☒ Enable TLS 1.2 ☒ Enable TLS 1.1 ☒ Enable TLS 1.0 ☐ Enable SSL 3.0																																			
CVM Access Control ☐ CVM Port 8000 (Default: 8000) ☐ CVM SSL Port 8443 (Default: 8443)																																			
AP Management ☒ Enable AP Management ☒ Device Management ☐ Respond to external device																																			
OK																																			

Step 4: Configure Router B



4.1 Configure VLAN in Vigor2926 (B)

- **Connect your PC to Router LAN port 1**
- Log into the router using the IP address 192.168.1.1 (*username/password admin/admin*).
- Go to **LAN>>VLAN Configuration** menu.
- Select **Enable**.
- Select P1, P2, **P3 and P4** to be members of **VLAN1** and subnet **LAN 2**.
- Click **OK** to save the settings.

LAN >> VLAN Configuration

VLAN Configuration

☒ Enable

	LAN				Subnet	VLAN Tag		
	P1	P2	P3	P4		Enable	VID	Priority
VLAN0	☐	☐	☐	☐	LAN 1 ▼	☐	0	0 ▼
VLAN1	☒	☒	☒	☒	LAN 2 ▼	☐	0	0 ▼
VLAN2	☐	☐	☐	☐	LAN 1 ▼	☐	0	0 ▼
VLAN3	☐	☐	☐	☐	LAN 1 ▼	☐	0	0 ▼
VLAN4	☐	☐	☐	☐	LAN 1 ▼	☐	0	0 ▼
VLAN5	☐	☐	☐	☐	LAN 1 ▼	☐	0	0 ▼
VLAN6	☐	☐	☐	☐	LAN 1 ▼	☐	0	0 ▼
VLAN7	☐	☐	☐	☐	LAN 1 ▼	☐	0	0 ▼
VLAN8	☐	☐	☐	☐	LAN 1 ▼	☐	0	0 ▼
VLAN9	☐	☐	☐	☐	LAN 1 ▼	☐	0	0 ▼
VLAN10	☐	☐	☐	☐	LAN 1 ▼	☐	0	0 ▼
VLAN11	☐	☐	☐	☐	LAN 1 ▼	☐	0	0 ▼
VLAN12	☐	☐	☐	☐	LAN 1 ▼	☐	0	0 ▼
VLAN13	☐	☐	☐	☐	LAN 1 ▼	☐	0	0 ▼
VLAN14	☐	☐	☐	☐	LAN 1 ▼	☐	0	0 ▼
VLAN15	☐	☐	☐	☐	LAN 1 ▼	☐	0	0 ▼

☒ Permit untagged device in P1 to access router

Note:

1. For each VLAN row, selecting Enable VLAN Tag will apply the associated VID to the selected wired LAN port.
2. Each VID must be unique.

OK Clear Cancel

4.2 Configure LAN Subnet in Vigor2926 (B)

4.2.1 Configure LAN 2

- Log into the router using the IP address 192.168.2.1 (Since we changed the ports to belong to LAN 2 in the previous step)
- Go to **LAN>>General Setup** Configuration menu.
- Click on **Details Page** button for LAN 2.

LAN >> General Setup

General Setup

Index	Status	DHCP	IP Address		
LAN 1	V	V	192.168.1.1	Details Page	IPv6
LAN 2	☒	☒	192.168.2.1	Details Page	IPv6
LAN 3	☐	☒	192.168.3.1	Details Page	IPv6

- Enter the LAN IP address 172.17.2.1
- Select **"For Routing Usage"** option
- Enter DHCP settings as shown below:
 - Enable Server
 - Start IP Address: 172.17.2.10
 - IP Pool Counts: 100
 - Gateway IP Address: 172.17.2.1
- Click **OK** to save settings (The router may reboot to save and activate the new settings).

LAN >> General Setup

LAN 2 Ethernet TCP / IP and DHCP Setup

Network Configuration

☒ Enable
 ☐ Disable
 ☐ For NAT Usage
 ☒ For Routing Usage

IP Address: 172.17.2.1

Subnet Mask: 255.255.255.0

LAN 2 IPv6 Setup

DHCP Server Configuration

☐ Disable
 ☒ Enable Server
 ☐ Enable Relay Agent

Start IP Address: 172.17.2.10

IP Pool Counts: 100 (max. 1021)

Gateway IP Address: 172.17.2.1

Lease Time: 259200 (s)

☒ Clear DHCP lease for inactive clients periodically.

DNS Server IP Address

Primary IP Address:

Secondary IP Address:

Note: Change IP Address or Subnet Mask in Network Configuration will also change HA LAN2 Virtual IP to the same domain IP.

OK

Once completed, the LAN settings should appear as shown below:

LAN >> General Setup

General Setup

Index	Status	DHCP	IP Address		
LAN 1	V	V	192.168.1.1	Details Page	IPv6
LAN 2	☒	☒	172.17.2.1	Details Page	IPv6
LAN 3	☐	☒	192.168.3.1	Details Page	IPv6

Step 5: Configure WAN 1 – Router B

- Log into the router using the IP address 172.17.2.1
- Go to WAN >> Internet Access menu
- Select **Static or Dynamic IP** for WAN 1
- Click on Details Page button for WAN 1

WAN >> Internet Access

Internet Access

Index	Display Name	Physical Mode	Access Mode		
WAN1		Ethernet	Static or Dynamic IP	Details Page	IPv6
WAN2		Ethernet	Static or Dynamic IP	Details Page	IPv6
WAN3		USB	None	Details Page	IPv6
WAN4		USB	None	Details Page	IPv6

Note:

- Select **Enable**
- Select **Enable RIP** for “RIP Protocol “setting
- Select Specify an IP address
- Enter IP address 172.168.1.2, Netmask: 255.255.255.0, Gateway 172.168.1.1

WAN >> Internet Access

WAN 1

PPPoE	Static or Dynamic IP	PPTP/L2TP	IPv6	
☒ Enable ☐ Disable	Keep WAN Connection ☐ Enable PING to keep alive PING to the IP PING Interval minute(s) WAN Connection Detection Mode ARP Detect MTU 1500 (Max:1500) Path MTU Discovery Detect RIP Protocol ☒ Enable RIP Bridge Mode ☐ Enable Bridge Mode Bridge Subnet LAN 1 BPA Setup (For Australia Only) ☐ BPA Enable Login Server not select	WAN IP Network Settings WAN IP Alias ☐ Obtain an IP address automatically Router Name Vigor Domain Name ☐ DHCP Client Identifier * Username Password ☒ Specify an IP address IP Address 172.168.1.2 Subnet Mask 255.255.255.0 Gateway IP Address 172.168.1.1 ☐ Default MAC Address ☐ Specify a MAC Address MAC Address: 00 1D AA AC 93 D9 DNS Server IP Address Primary IP Address 8.8.8.8 Secondary IP Address 8.8.4.4		

Step 6: Enable Remote Management in Router A

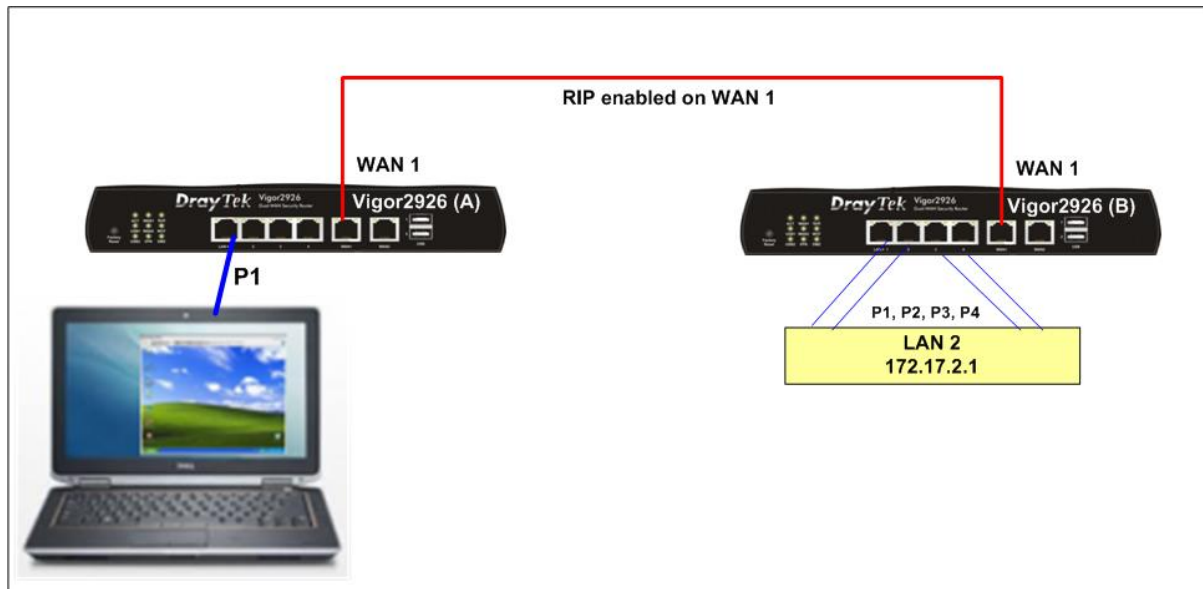
- Log into the router using the IP address 172.17.2.1
- Go to **System Maintenance >> Management** menu in the router.
- Enter the settings as shown below:
 - Select **Allow management from the Internet**
 - Select **HTTP Server**
 - Deselect **Disable PING from the Internet**
 - Click **OK** to save (*Router will restart to save the settings*)

System Maintenance >> Management

IPv4 Management Setup	IPv6 Management Setup	LAN Access Setup																																	
Router Name: DrayTek																																			
☐ Default: Disable Auto-Logout ☐ Enable Validation Code in Internet/LAN Access																																			
Internet Access Control ☒ Allow management from the Internet Domain name allowed:																																			
☐ FTP Server ☒ HTTP Server ☐ Enforce HTTPS Access ☒ HTTPS Server ☐ Telnet Server ☐ TR069 Server ☐ SSH Server ☐ SNMP Server ☐ Disable PING from the Internet																																			
Access List from the Internet <table border="1"> <thead> <tr> <th>List</th> <th>index in IP Object</th> <th>IP / Mask</th> </tr> </thead> <tbody> <tr><td>1</td><td></td><td></td></tr> <tr><td>2</td><td></td><td></td></tr> <tr><td>3</td><td></td><td></td></tr> <tr><td>4</td><td></td><td></td></tr> <tr><td>5</td><td></td><td></td></tr> <tr><td>6</td><td></td><td></td></tr> <tr><td>7</td><td></td><td></td></tr> <tr><td>8</td><td></td><td></td></tr> <tr><td>9</td><td></td><td></td></tr> <tr><td>10</td><td></td><td></td></tr> </tbody> </table>			List	index in IP Object	IP / Mask	1			2			3			4			5			6			7			8			9			10		
List	index in IP Object	IP / Mask																																	
1																																			
2																																			
3																																			
4																																			
5																																			
6																																			
7																																			
8																																			
9																																			
10																																			
Management Port Setup ☒ User Define Ports ☐ Default Ports Telnet Port: 23 (Default: 23) HTTP Port: 80 (Default: 80) HTTPS Port: 443 (Default: 443) FTP Port: 21 (Default: 21) TR069 Port: 8069 (Default: 8069) SSH Port: 22 (Default: 22)																																			
Brute Force Protection ☐ Enable brute force login protection ☐ FTP Server ☐ HTTP Server ☐ HTTPS Server ☐ Telnet Server ☐ TR069 Server ☐ SSH Server Maximum login failures: 0 times Penalty period: 0 seconds																																			
Blocked IP List																																			
TLS/SSL Encryption Setup ☒ Enable TLS 1.2 ☒ Enable TLS 1.1 ☒ Enable TLS 1.0 ☐ Enable SSL 3.0																																			
CVM Access Control ☐ CVM Port: 8000 (Default: 8000) ☐ CVM SSL Port: 8443 (Default: 8443)																																			
AP Management ☒ Enable AP Management ☒ Device Management ☐ Respond to external device																																			
OK																																			

Step 7: Connect the two Routers and Test

Connect WAN 1 of Router A to WAN 1 of router B using an Ethernet cable as shown in the diagram below and connect your laptop to LAN port P1 of router A.



Check the Online Status page of Router A to verify that the two routers are connected. You should see WAN 1 status as enabled and running.

DrayTek Vigor2926 Series

Auto Logout | IPv6

Dashboard
Wizards
Online Status
Physical Connection
Virtual WAN

WAN
LAN
Hotspot Web Portal
Routing
NAT
Hardware Acceleration
Firewall
User Management
Objects Setting
CSM
Bandwidth Management
Applications
VPN and Remote Access
Certificate Management
SSL VPN
USB Application

Online Status

Physical Connection System Uptime: 0day 1:28:27

IPv4		IPv6	
LAN Status			
IP Address	TX Packets	RX Packets	Router Primary DNS: Router Secondary DNS:
192.168.1.1	2,365	2,072	8.8.8.8 8.8.4.4
WAN 1 Status			
Enable	Line	Name	Mode Up Time
Yes	Ethernet		Static IP 0:01:32
IP	GW IP	TX Bytes	TX Rate(Kbps) RX Bytes RX Rate(bps)
172.168.1.1	172.168.1.2	69 (KB)	3.22 1138 (B) 24
WAN 2 Status >> Renew			
Enable	Line	Name	Mode Up Time
Yes	Ethernet		DHCP Client 00:00:00
IP	GW IP	TX Bytes	TX Rate(bps) RX Bytes RX Rate(bps)
---	---	0 (B)	0 0 (B) 0

7.1 Check the Routing Tables

Go to **Diagnostics >> Routing Table** menu in each router and check the routing tables. You should see one route is using RIP protocol (Have **R** in left column next to the route).

Router A

DrayTek Vigor2926 Series

Diagnostics >> View Routing Table

IPv4

Key	Destination	Gateway	Interface
*	0.0.0.0/ 0.0.0.0	via 172.168.1.2	WAN1
C	172.168.1.0/ 255.255.255.0	directly connected	WAN1
C~	192.168.1.0/ 255.255.255.0	directly connected	LAN1
C	192.168.2.0/ 255.255.255.0	directly connected	LAN2
R	172.17.2.0/ 255.255.255.0	via 172.168.1.2	WAN1 (2/90000)

Key
C: Connected S: Static R: RIP *: default ~: private B: BGP

Router B

DrayTek Vigor2926 Series

Diagnostics >> View Routing Table

IPv4

Key	Destination	Gateway	Interface
*	0.0.0.0/ 0.0.0.0	via 172.168.1.1	WAN1
C	172.168.1.0/ 255.255.255.0	directly connected	WAN1
C~	192.168.1.0/ 255.255.255.0	directly connected	LAN1
R	192.168.2.0/ 255.255.255.0	via 172.168.1.1	WAN1 (2/89010)
C	172.17.2.0/ 255.255.255.0	directly connected	LAN2

Key
C: Connected S: Static R: RIP *: default ~: private B: BGP

Step 8: Test Connectivity

Since we have enabled remote access to both routers and enabled ping from the Internet you should be able to access and ping each router as well as the routed LANs.

8.1 Test from router A to router B

With your PC connected to any LAN ports in **router A** you should be able to ping the routed LAN (LAN 2 - 172.17.2.1) on router B. You should also be able to connect to router B using a web browser.

- Connect to router B using both 172.17.2.1 and 172.168.1.2 addresses (you should get the router login page to appear).

8.2 Test from router B to router A

You can repeat the above in the reverse direction. i.e. with your PC connected to any LAN port in router B and test connectivity to router A.

- Connect to router A using both 192.168.2.1 and 172.168.1.1 addresses (you should get the router login page to appear).

8.3 Additional exercise

If time permits, attach an access point or another device to a LAN port on router B and you should be able to access it from router A.