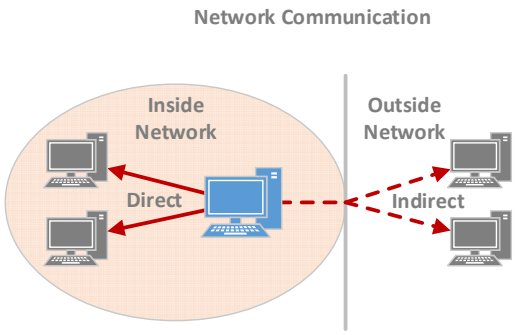
Assignment Introduction

The objective of this assignment is for you to learn the basics of IPv4 routing. While routing is defined for many protocols and models, such as OSI model routing, IPv6 routing, and public switched telephone network (PSTN) routing, this assignment focuses exclusively on teaching you routing as it pertains to IPv4 models and protocols. As such, please keep in mind that words and concepts that may generically apply to many protocols and models, such as "routers", "routing", and "networks", are defined and used in this assignment exclusively in the context of IPv4 networks and protocols.

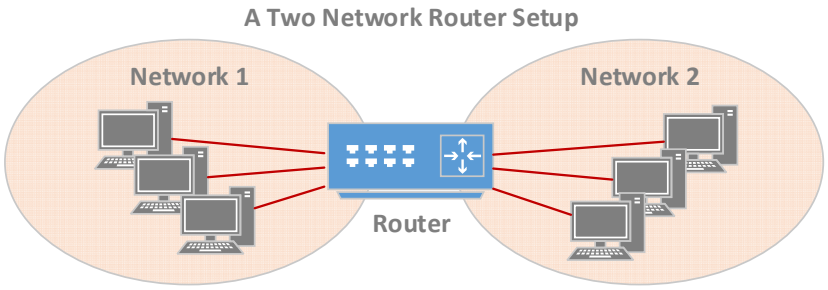
Section One – Foundational Routing Concepts

Let us first review some fundamental networking concepts. IPv4 operates at the network layer, and introduces the network concept into the five-layer Internet model. A network in this context can be casually defined as a group of devices and computers that communicate directly in the group and indirectly with devices and computers not in the group, creating a virtual boundary that demarcates direct and indirect communication. This concept is illustrated in the figure below.

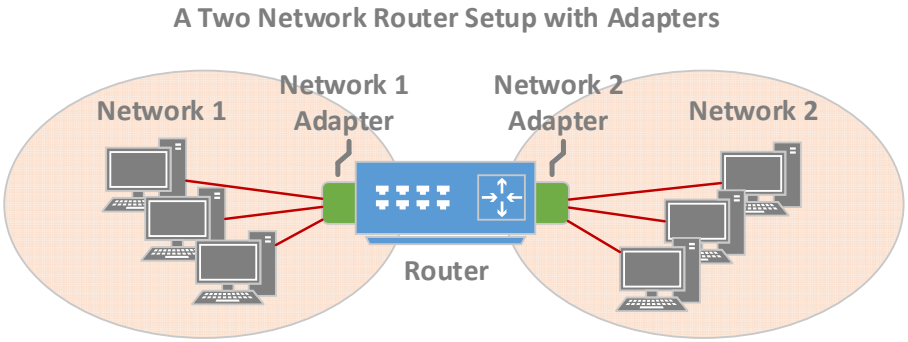


With direct communication, the sender directly addresses the receiver at the data-link layer, and the networking devices and cables on the network are configured so that frames from the sender arrive at the receiver.

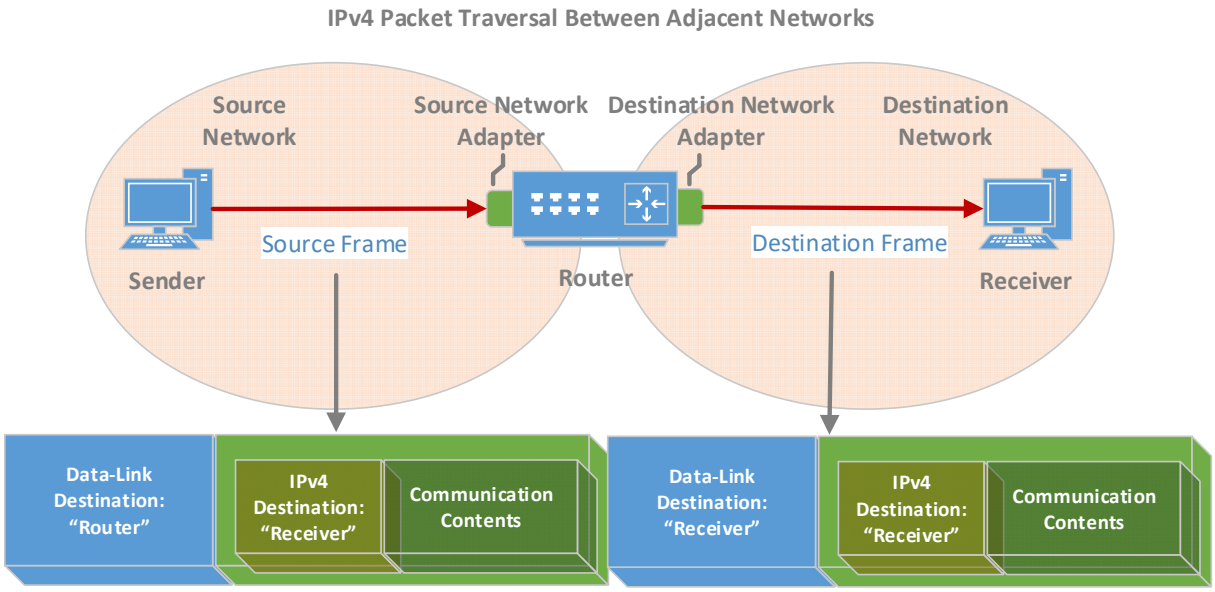
We see two layers at work in host-to-host communication. A host can communicate directly with another host on the same network at the data-link layer, but can only communicate with a host on a different network through the network layer. The data-link layer supports intranetwork communication, and the network layer supports internetwork communication. In particular, a host relies on routing with IPv4 in order to communicate with hosts outside of its own network. *IPv4 routing* is the process of moving an IPv4 packet from the sender to the receiver. The sending host initiates the routing process, then relies on IPv4 routers to move the communication to the receiver's network. An *IPv4 router* is a device that connects two or more IPv4 networks together. The following figure illustrates a router that connects two adjacent networks together.



Whereas a client computer is only able to directly communicate with hosts on its own network, a router can communicate with hosts on all of the networks it is directly connected to. How can it do this? Simple! A router has one network adapter for each network, and because each adapter is assigned its own MAC and IPv4 address, each adapter is configured to function on a different network. If the router is connected to two networks as illustrated in the previous figure – Network 1 and Network 2 – hosts on Network 1 send messages to the router's Network 1 adapter, and hosts on Network 2 send messages to the router's Network 2 adapter. This is illustrated in the following figure.



IPv4 packets traverse adjacent networks as follows. When a host needs to send an IPv4 packet to a host outside of its own network, it embeds the packet into a data-link layer frame, and addresses the frame to the router's network adapter that is configured to participate on its network. Unlike a client computer, when a router receives a data-link layer frame, it expects that the embedded IPv4 packet may not be addressed to it directly, but may be intended for another host. It therefore extracts the IPv4 packet from the frame and inspects the IPv4 destination address. If the packet is indeed destined for another host on a different network, the router creates a new data-link layer frame with the destination host's MAC address as the destination address, embeds the IPv4 packet in it, and then sends the frame out of the network adapter corresponding to the destination network. In this way, the router bridges two or more networks together. The following figure illustrates IPv4 packet traversal between two adjacent networks.

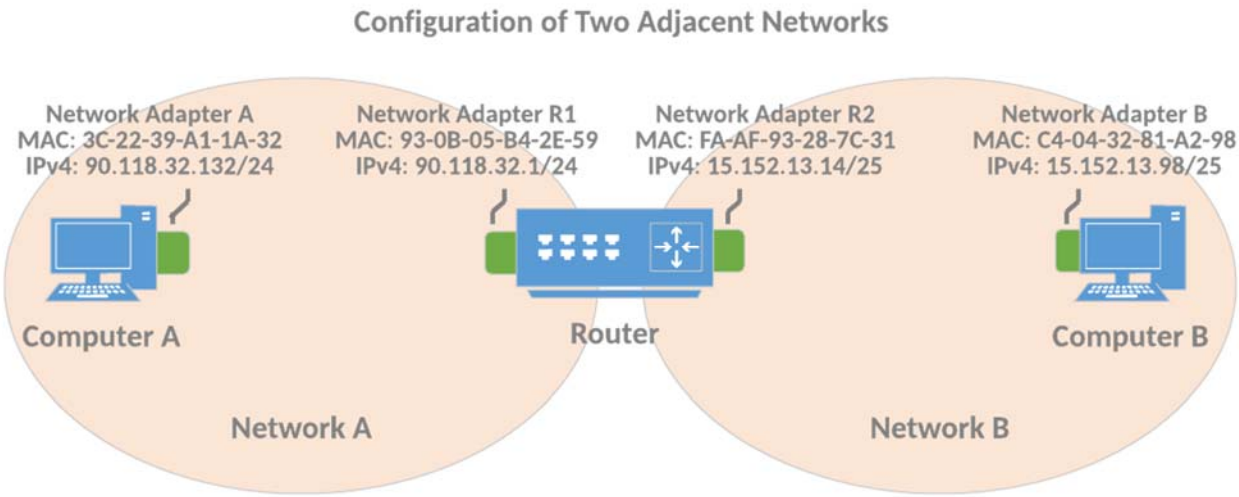


Notice that the sender sends the frame to the router's network adapter configured for its own network, and that the router sends out a new frame out of its network adapter configured for the destination network, which is addressed to the receiver. Further notice that the IPv4 packet embedded inside of each frame starts out and remains addressed to the receiver. Keep in mind that the data-link layer only makes use of the data-link address, most commonly a MAC address, and the network layer only makes use of the network address, most commonly an IPv4 address.

It is important for us to understand that although IPv4 routing is a network layer function, the data-link layer also plays a role in routing. In particular, the data-link layer is always used to transmit an IPv4 packet, whether the packet is being sent directly to the receiver, or is being sent to a router. When the sender and receiver are on the same network, the sender directly transmits the IPv4 packet to the receiver via the data-link layer. When the sender and receiver are on a different network, the sender forwards the IPv4 packet to the router via the data-link layer, and ultimately the router on the receiver's network transmits the IPv4 packet to the receiver via the data-link layer. The network layer decides which host (technically, which network adapter) should receive the packet, and the data-link layer transmits it to that host.

Now that we have reviewed several important routing concepts, you have a chance to apply what you have learned thus far in Scenario 1.

Scenario 1: Adjacent Network Configuration
Imagine that two networks – Network A and Network B -- are adjacent to each other and are connected with a single router., Further imagine that the MAC and IPv4 addresses of each network adapter are configured as illustrated in the following figure.



1. Identify which adapter(s) would receive a data-link layer broadcast transmitted by Computer B and which would not (if any). Provide an explanation of why *each adapter present in the preceding figure* would or would not receive the broadcast.

2. Can Computer B directly address Computer A at the data-link layer? Explain why or why not.

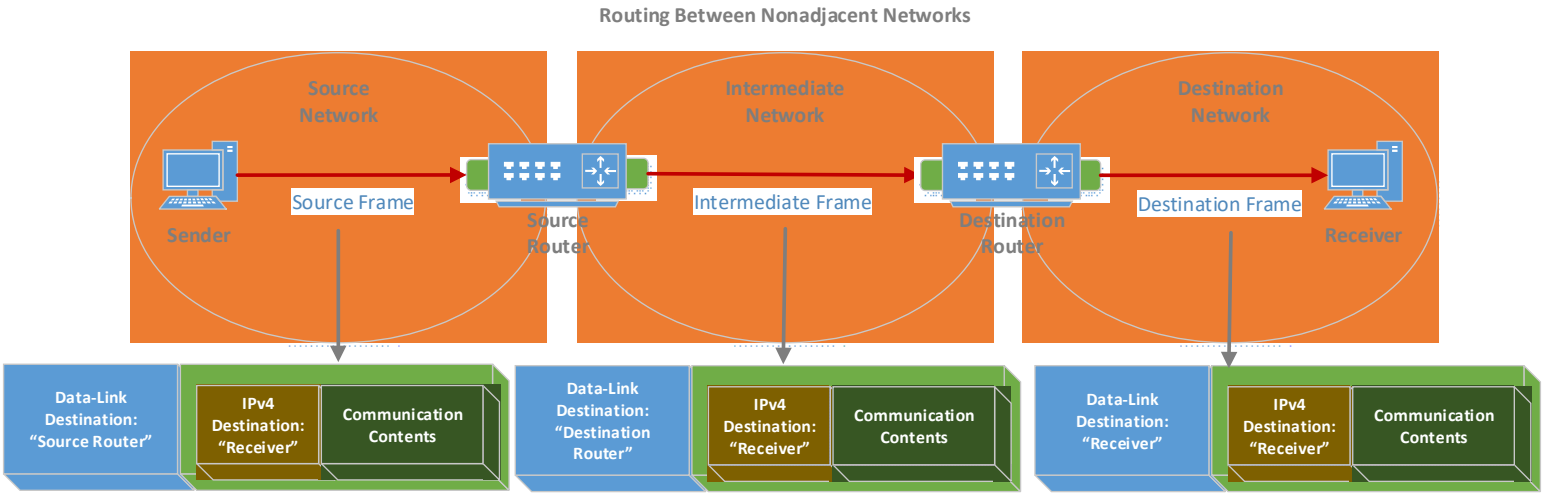
3. Imagine that Computer B successfully transmits an IPv4 packet to Computer A, that there are no errors on any frame or packet, and that the ARP cache on all computers and the router is already fully populated. Identify any data-link layer frame(s) that are created for this transmission. For each frame, identify the adapter it originates from and the adapter it is addressed to, explain why it was created, and provide its source and destination MAC address and source and destination IPv4 address.

4. What function does the router serve for the transmission in #3?

Routing Between Non-Adjacent Networks
A sender and receiver are not always on adjacent networks. In such a case, the first router to receive the IPv4 packet routes it to another router, which in turn routes it to another, until the router on the destination network receives the packet. The router then forwards the packet to the receiver by addressing the receiver directly at the data-link layer. If a router has a network adapter configured to be on the same network as the receiver, the router sends it to the receiver directly; otherwise, the router routes the packet to another router. Thus the IPv4 packet is routed from network to network until it arrives at the destination network.

Routing between nonadjacent networks with one intermediate network in-between is illustrated in

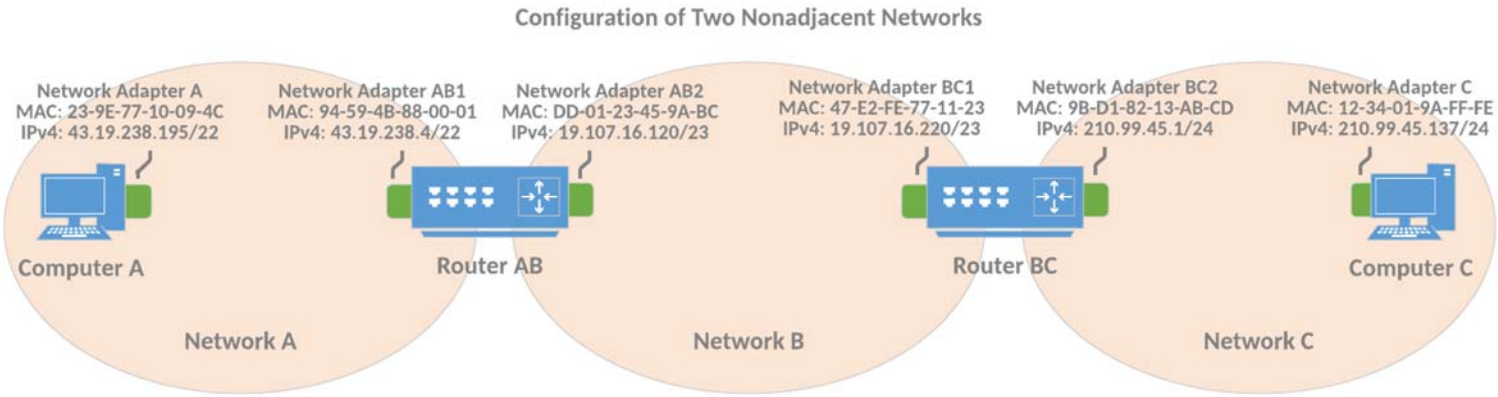
the following figure.



Notice that the sender addresses the frame to the source router, the source router creates an intermediate frame and addresses it to the destination router, and finally the destination router addresses the receiver directly. Further notice that the embedded IPv4 packet starts out and remains addressed to the receiver. Thus routing enables an IPv4 packet to travel from network to network until it arrives at the destination network. You apply this knowledge in Scenario 2.

Scenario 2: Routing Between Nonadjacent Networks

Imagine that three networks – Network A, Network B, and Network C -- are connected to each other with one router between Network A and Network B, and another router between Network B and Network C. Further imagine, and that the MAC and IPv4 addresses of each network adapter are configured as illustrated in the following figure.



5. Imagine that Computer C successfully sends an IPv4 packet to Computer A, that there are no errors on any frame or packet during the transmission, and that the ARP cache on all computers and routers has been fully populated before the packet is sent. Identify any data-link layer frame(s) that are created in this scenario. For each frame, identify the adapter it originates from and the adapter it is addressed to, explain why it was created, and provide its source and destination MAC address and source and destination IPv4 address.

6. Across all frames in the transmission in #5, contrast the number of different destination IP addresses with the number of different MAC addresses. Why are these numbers different, and what does this tell us about the routing process?

Section Two - Routing Tables

You may be wondering how a host or router determines where to transmit an IPv4 packet, especially because any particular network can contain dozens, hundreds, or thousands of hosts, and the answer lies in the routing table. A *routing table* is a set of rules used by a host to formulaically determine the next-hop destination of an IPv4 packet. In particular, each host uses its routing table to determine which of its network adapters it will use for the transmission, and which host (technically, which network adapter) will be the next-hop recipient. The term "table" in "routing table" is used primarily because the set of rules defined in a routing table is most often displayed in a tabular format, which consists of specific columns information, with one rule per row. Each rule defines the next hop for a particular network as defined by a network address and a subnet mask. Computers and devices are concerned with the rules themselves, and we as human beings view the rules in a tabular format, for understandability. A routing table contains all the information necessary for a host to determine where transmit an IPv4 packet.

It is important to understand that routing a packet from a sender to a receiver is distinct from a routing protocol. A *routing protocol* specifies exactly how routers share route information with each other, so that routers are able to communicate and configure their routing tables. Routing protocols treat each network as a single entity, and therefore exclusively consider networks, but not hosts on the network, when computing routes. Routing, on the other hand, uses the route information defined by a routing protocol, or route information defined through some other means such as manual or DHCP route assignment, in order to move an IPv4 packet from a sender to a receiver. A router may settle upon a set of routes by using a routing protocol, then route a copious number of packets using that set of routes. There are many different routing protocols in use today, but they all perform the same function – to determine viable and efficient routes for IPv4 packets, and to update the routing table on each router to reflect this.

Let us take a look at the structure of a routing table. The significant columns of information in a routing table are the destination network's network address, the destination network's subnet mask, the network adapter to be used to reach the destination network, the IPv4 address of the next hop to reach for the destination network, and a metric that is used to determine which rule is preferable in the event two or more rules can be used. Each of these is explained in turn below.

The Destination Network's Network Address

What it Means: The network address is specified in this column so that the sending host knows which network is specified by the rule. Recall that a network can contain many hosts, and so any one rule in a routing table can identify the next-hop recipient for all hosts in a network.

Example: 35.26.1.0 is an example of a network address.

Common Title: When routing tables are printed, you will often see this column titled "Network Destination" or "Destination", though different operating systems and tools may use a different title.

The Destination Network's Subnet Mask

What it Means: The subnet mask determines which of the bits in an IPv4 address are used in the network identifier, and which are used in the host identifier. Recall that the network identifier

uniquely identifies a particular network, and the host identifier uniquely identifies a host on that network.
Example: 255.255.252.0 is an example of a subnet mask.

How it Works: The sending host collectively uses the destination network's address and subnet mask to determine if a particular IPv4 address matches a rule. For example, given a destination IPv4 address of 192.168.1.0, a rule with network address 192.168.1.0 and subnet mask 255.255.255.0 matches the destination address, but a rule with network address 192.168.5.0 and subnet mask 255.255.255.0 does not match the destination address.

It is important to note that if an IPv4 address matches two or more rules, the most specific rule – the one with the most number of 1 bits in the subnet mask – is the rule that is IPv4 uses to determine the next hop. For example, if one matching rule specifies 10.0.0.0/8 for its network address and subnet mask, and a second matching rule specifies 10.2.8.0/24, the second matching rule wins. You may now legitimately wonder what happens when two or more rules may match the same IPv4 address *and* also have the same number of 1 bits in the subnet mask. In such a case, another piece of information in the routing table – the metric – is used to settle the dispute. The metric is discussed in more detail in its own section, so you may refer to that section for more details. Because more than one rule may match any particular IPv4 address, it is important that one of the rules still wins so that the host definitely decides on the next hop.

This selection process makes way for the most generic of all possible network address and subnet mask pairs, the default route, which is uses 0.0.0.0/0. Clearly, all IPv4 addresses match this pair (think about this carefully until you are sure this is the case). A *default route* is a rule that takes effect when no other rule matches. Client computer configurations commonly utilize the default route to reach the only router available on their network, so that all communications intended for hosts outside of its own network are transmitted to that router. This limits the routing options for a client computer to two – either send it to a host on the same network, or send it to the router on the network. Routers are also commonly configured with a default route. The default route provides a mechanism for hosts to always have a matching rule for all IPv4 addresses.

Although we describe a rule with specification 0.0.0.0/0 as the default route, the host with the routing table need not perform special logic to use the rule. It simply uses the same methodology it uses for all IPv4 addresses, which is the find all rules that match the IPv4 address, then select the one rule that has the most number of 1 bits for the subnet mask, or the rule with the best metric in case of a tie. We classify the rule for our understanding, but the host simply uses the rule as it would any other. The methodology used by the host ensures that it will use a more specific rule when it is able to, and the default route otherwise.

Common Title: You will often see this column titled "Netmask" or "Genmask", though different operating systems and tools may use a different title.

The IPv4 Address of the Next Hop
What it Means: There is always a next-hop destination in the process of routing an IPv4 packet. The next hop may be the final destination, or it may be a router which is able to directly or indirectly reach the final destination. The host transmitting the IPv4 packet relies on the rules present in the routing

table to make this determination, and the most preferred matching rule determines which host (technically, which adapter) will receive the IPv4 packet, and that host is identified with its IPv4 address.

There are two categories of the next hop – an actual host, or a specification that the final destination is directly reachable on the network – and the category determines what value is placed in this next-hop column. If the final destination *is not* on the same network as the host sending the IPv4 packet, the next hop will be a router, and the IPv4 address of the router is specified in the next hop column. If the final destination *is* on the same network as the sending host, the next hop is the final destination itself, in which case the sending host need not forward the packet to a router. In such a case, either the IPv4 address of the *sending* host is placed in the next hop column, or a special value such as "On-link" is used. Regardless of the value that is printed in the routing table by the operating system or tool, the sending computer knows that the host is directly reachable and can be addressed directly at the data-link layer. The value displayed in the routing table is for human benefit only. The two categories of the next hop determines what is printed in the routing table and whether the sending host forwards the packet to a router, or sends it directly to the final destination.

Example: 32.35.1.215 is an example of a next-hop IPv4 address, in the case where it is a router. "On-link" is an example of the case when the final destination is directly reachable on the same network.

Common Title: You will often see this column title "Gateway", though different operating systems and tools may use a different title. It is important to note that, although the term "gateway" is used, the next hop will be a client host or a router, and very rarely is the next hop an actual gateway in the technical sense of the word, a router capable of translating in-between different protocols.

The Network Adapter to be Used

What is Means: Each host on a network has at least one network adapter which enables it to communicate on the network. Each rule in the routing table must specify which of the available network adapters will be used to transmit an IPv4 packet, so that the host can use the correct adapter in the event the rule is selected as the most preferable match for an IPv4 address. Client computers commonly have one physical network adapter, though they can be configured with more than one, and routers commonly have two or more physical network adapters. Hosts are also commonly configured with a virtual network adapter which represents the host itself on the network, so that a host can send communications to itself without the need to utilize the full TCP/IP stack. This virtual network adapter is often given the title "localhost" and the IPv4 address 127.0.0.1.

Example: While we may ascribe very simple identifiers to our network adapters, such as "Network Adapter 1", the operating system assigns more technical identifiers. For example, the Windows operating system assigns numbers such as "16" or "12" as an identifier, and the Linux operating system assigns titles that represent the technology and a unique number, such as "eth0" to represent the first Ethernet-capable network adapter on the host. To add to this complexity, some operating systems and tools will display the IPv4 address assigned to a network adapter in the routing table, rather than its technical title, while others will display the technical title. It is most important for you to understand that each network adapter is uniquely identified by the operating system, and that each rule in a routing table designates which network adapter is to be used for transmitting an IPv4 packet.

Common Title: You will often see this column titled “Interface” or “Use Iface”, though different operating systems and tools may use a different title.

Metric

What it Means: Because it is possible that a destination IPv4 address matches two or more rules with the same number of 1 bits for the subnet mask, the metric is used as a discriminator which indicates the more preferable rule. The value is stored as a number, and what the number means depends upon the particulars of the routing configuration on the host. The value may be the number of hops needed to reach a destination, so that a route with fewer hops will be preferred, but the value is more often a relative value that has no intrinsic meaning. Routing protocols use many strategies to determine the best routes, and a strategy may include the number of hops, the overall travel time, other factors, or a combination of any or all of these. Regardless of what the metric literally means, a better metric indicates to the host that it should prefer that rule over others when there is otherwise a tie.

You may reasonably wonder what happens when two or more rules match an IPv4 address, have the same number of 1 bits for the subnet mask, *and* have the same metric value. The answer to this is, it depends upon the particulars of the computer or device. Some hosts will use the rules alternately, effectively load balancing the packets between the matching routes. It is necessary to read the vendor specific documentation to determine what occurs in this case for any particular operating system and device.

Example: A metric of “1” may mean a lower cost rule, and a metric of “10” may mean a higher cost rule; however, a higher number may be preferable to a lower number. The host’s operating system, or the routing protocol in use on the host, defines how the metric is calculated.

Common Title: You will often see this column titled “Metric”, though different operating systems and tools may use a different title.

Let us now take a look at an example routing table rule.

Network Destination	Netmask	Gateway	Interface	Metric
153.23.16.0	255.255.255.0	153.23.16.1	eth0	10

This rule tells the host that any address that matches the 153.23.16.0/24 network is to be transmitted by the network adapter “eth0”, and is to be sent to the host (technically, network adapter) with IPv4 address 153.23.16.1. See, now that you understand a routing table’s components, the explanation of what the rule means is not complicated. So, IPv4 address 153.23.16.19 would match this rule, but IPv4 addresses 19.32.0.19 and even 153.23.14.1 would not match this rule.

Taking the previous example, now let us dive into one more detail which is very important. Which host has the gateway address of 153.23.16.1 determines whether the rule is indicating that the next hop is a router, or the next hop is the final destination (i.e. that the host with the routing table is on the same network as the final destination). If 153.23.16.1 *is not* the address of the sending host, the next hop is a router. If 153.23.16.1 *is* the address of the host with the routing table, the next hop is the final destination (i.e. the intended receiver of the packet). In the latter case, the host will not attempt to forward to packet to the gateway address, but will address the final destination host directly at the

data-link layer. Some operating systems use another designation in the Gateway column, such as “On-link”, to indicate that any hosts that match the rule can be reached directly by the host. So one class of rules in a routing table indicate that the next hop is a router, and the other class indicates that the next hop is the final destination and therefore the receiver is directly addressable, and the class can be determined by the value in the Gateway column.

Just so we can be sure that this point is clear, let us look a sample routing table of a client computer. Imagine that a host has IPv4 address 192.168.1.30, and that it has a routing table as follows.

Network Destination	Netmask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	192.168.1.1	eth0	10
192.168.1.0	255.255.255.0	192.168.1.30 *or* “On-link”	eth0	10

The first rule is the default route, which indicates that if any other rules do not match, the IPv4 packet is to be forward to the router with IPv4 address 192.168.1.1. You can discern that it is the default route because of the 0.0.0.0/0 specification. The second rule indicates the next hop is on the same network as the host and can therefore be addressed directly. Why? Because the gateway column of the second rule indicates the same address as the host, or some other indicator such as “On-link”. Of course, the host internally knows whether the destination address is considered “On-link” or not in a different manner, but this is the way it is displayed in the routing table. So, if the host needs to send an IPv4 packet to address 10.2.3.9, it is going to forward the IPv4 packet to the router with address 192.168.1.1, because it does not match the second rule, and so it uses the first rule as the default route. If the host needs to send an IPv4 packet to address 192.168.1.215, it will directly address that host at the data-link layer, because it is directly reachable.

Let us look at a sample routing table of a router which has two network adapters which are configured with 192.168.1.1/24 and 10.2.8.1/16.

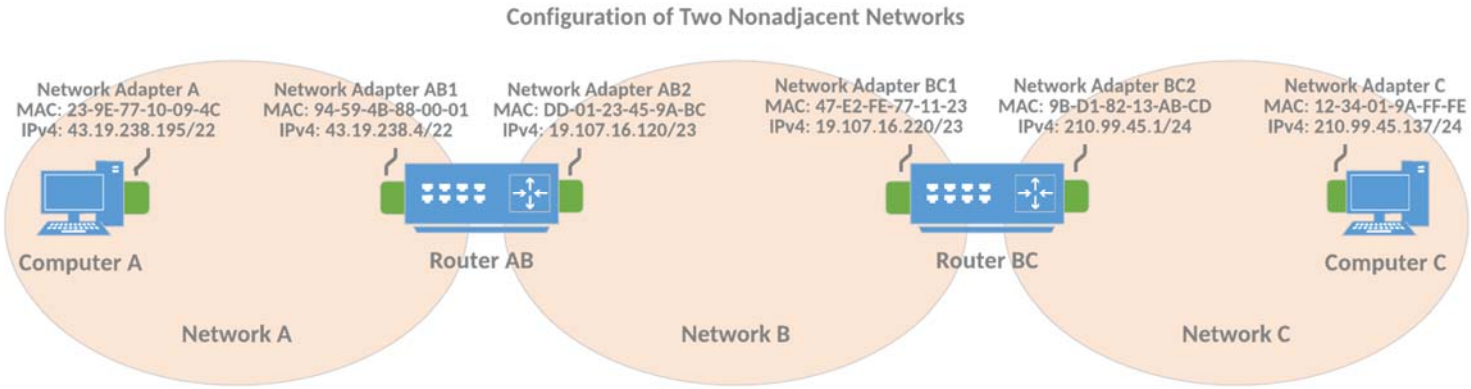
Network Destination	Netmask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	192.168.1.254	adapter1	10
192.168.1.0	255.255.255.0	192.168.1.1 *or* “On-link”	adapter1	10
10.2.0.0	255.255.0.0	10.2.8.1 *or* “On-link”	adapter2	10

The first rule is the default route, and it indicates that if no other rules match, the router will forward the packet to another router with IPv4 address 192.168.1.254 over its first network adapter (adapter1). The second rule indicates that if any packet need be sent to any host on the 192.168.1.0/24 network, that host can be directly reached on adapter1. The third rule indicates that if any packet need be sent to any host on the 10.2.0.0/16 network, the host can be directly reached on adapter2.

Let us think about what these rules mean in terms of the router’s overall network configuration. The router is connected to two networks, 192.168.1.0/24 and 10.2.0.0/16, and can directly reach any host on those two networks over two different network adapters. If the packet is not destined for a host on either network, the router will forward the packet to another router with IPv4 address 192.168.1.254. A routing table is not hard to understand when broken down into its constituent parts.

Scenario 3: Creating Routing Table Rules

Here we will use the same network configuration as in Problem 2. Three networks – Network A, Network B, and Network C -- are connected to each other with one router between Network A and Network B, and another router between Network B and Network C. The MAC and IPv4 addresses of each network adapter are configured as illustrated in the following figure.



When you are asked to create routing table rules, make sure to specify the Network Destination, Netmask, Gateway, and Interface fields, and explain why each field's value has been chosen in your answer. You do not need to include the Metric field, since metric specifics can only be determined with knowledge of the specifics of a computer's environment. You may use the titles given in the figure for the network adapter specifications in the routing table.

7. To get started, calculate the network address and subnet mask of all three networks in this scenario. You will need these values to create rules for the computer's routing table.

8. Create a routing table for Computer C that has no default route, and that supports sending packets to all hosts (directly or indirectly) on Network A, Network B, and Network C. A hint is that this routing table will contain three rules.

9. Create a routing table for Computer C that has a default route, and that supports sending packets to all hosts (directly or indirectly) on Network A, Network B, and Network C. Make sure to remove redundant routes that are not necessary with the presence of a default route.

10. Would you recommend using the routing table in #8 or in #9, for Computer C? Explain why.

11. Create a routing table for Router AB which has no default route, which supports communications to all hosts (directly or indirectly) on Network A, Network B, and Network C. A hint is that this routing table will contain three rules.