OSI Network Layer

Network Fundamentals – Chapter 5

Cisco | Networking Academy®
Mind Wide Open™

Objectives

Identify the role of the Network Layer, as it describes communication from one end device to another end device

Examine the most common Network Layer protocol, Internet Protocol (IP), and its features for providing connectionless and best-effort service

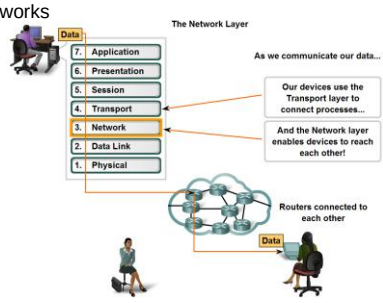
Understand the principles used to guide the division or grouping of devices into networks

Understand the hierarchical addressing of devices and how this allows communication between networks

Understand the fundamentals of routes, next hop addresses and packet forwarding to a destination network

Network Layer Protocols and Internet Protocol (IP)

Define the basic role of the Network Layer in data networks



The Network Layer

The Network layer, or OSI Layer 3, provides services to exchange the individual pieces of data over the network between identified end devices.

To accomplish this end-to-end transport, Layer 3 uses four basic processes:

1. Addressing
2. Encapsulation
3. Routing
4. Decapsulation

Addressing and Encapsulation

1. Addressing

If individual pieces of data are to be directed to an end device, that device must have a unique address.

In an IPv4 network, when this address is added to a device, the device is then referred to as a host.

2. Encapsulation

Second, the Network layer must provide encapsulation.

During the encapsulation process, Layer 3 receives the Layer 4 PDU and adds a Layer 3 header, or label, to create the Layer 3 PDU.

When referring to the Network layer, we call this PDU a packet.

When a packet is created, the header must contain, among other information, the address of the host to which it is being sent.

This is known as the destination address, but also includes the source address

IP Address Classes

Class A	1 – 127	(Network 127 is reserved for loopback and internal testing) Leading bit pattern	0	00000000.00000000.00000000.00000000 Network Host Host Host
Class B	128 – 191	Leading bit pattern	10	10000000.00000000.00000000.00000000 Network Network Host Host
Class C	192 – 223	Leading bit pattern	110	11000000.00000000.00000000.00000000 Network Network Network Host
Class D	224 – 239	(Reserved for multicast)		
Class E	240 – 255	(Reserved for experimental, used for research)		

Private Address Space

Class A	10.0.0.0 to 10.255.255.255
Class B	172.16.0.0 to 172.31.255.255
Class C	192.168.0.0 to 192.168.255.255

Default Subnet Masks

Class A	255.0.0.0
Class B	255.255.0.0
Class C	255.255.255.0

3. Routing

Next, the Network layer must provide services to direct these packets to their destination host.

Intermediary devices that connect the networks are called routers.

The role of the router is to select paths for and direct packets toward their destination. This process is known as routing.

During the routing through an internetwork, the packet may traverse many intermediary devices.

Each route that a packet takes to reach the next device is called a hop. As the packet is forwarded, its contents (the Transport layer PDU), remain intact until the destination host is reached.

4. Decapsulation

Finally, the packet arrives at the destination host and is processed at Layer 3.

The host examines the destination address to verify that the packet was addressed to this device.

If the address is correct, the packet is decapsulated by the Network layer and the Layer 4 PDU contained in the packet is passed up to the appropriate service at Transport layer.

Network layer protocols specify the packet structure and processing used to carry the data from one host to another host.

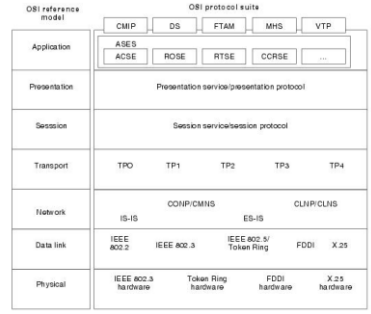
Each packet allows the Network layer to carry packets for multiple types of communications between multiple hosts.

Network Layer Protocols

7. Application
6. Presentation
5. Session
4. Transport
3. Network
2. Data Link
1. Physical

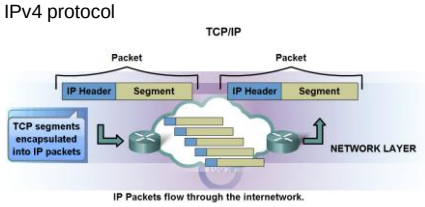
- Internet Protocol version 4 (IPv4)
- Internet Protocol version 6 (IPv6)
- Novell Internetwork Packet Exchange (IPX)
- AppleTalk
- Connectionless Network Service (CLNS/DECNet)

OSI Reference Model/Protocol Suite



Network Layer Protocols and Internet Protocol (IP)

Identify the basic characteristics and the role of the IPv4 protocol



IP Packets flow through the internetwork.

- Connectionless - No connection is established before sending data packets.
- Best Effort (unreliable) - No overhead is used to guarantee packet delivery.
- Media Independent - Operates independently of the medium carrying the data.

IPv4 and IPv6

The services provided by IP, as well as the packet header structure and contents, are specified by either IPv4 protocol or IPv6 protocol.

These services and packet structure are used to encapsulate UDP datagrams or TCP segments for their trip across an internetwork..

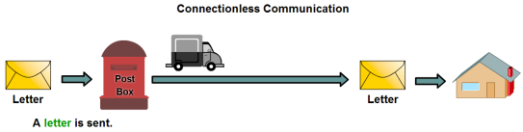
The Internet Protocol was designed as a protocol with low overhead.

It provides only the functions that are necessary to deliver a packet from a source to a destination over an interconnected system of networks.

The protocol was not designed to track and manage the flow of packets. These functions are performed by other protocols in other layers.

Network Layer Protocols and Internet Protocol (IP)

Describe the implications for the use of the IP protocol as it is connectionless



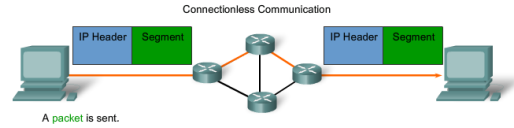
The sender doesn't know:

- if the receiver is present
- if the letter arrived
- if the receiver can read the letter

The receiver doesn't know:

- when it is coming

Data Network



The sender doesn't know:

- if the receiver is present
- if the packet arrived
- if the receiver can read the packet

The receiver doesn't know:

- when it is coming

IP as a Connectionless Protocol

Because IP is connectionless, it requires no initial exchange of control information to establish an end-to-end connection before packets are forwarded, nor does it require additional fields in the PDU header to maintain this connection.

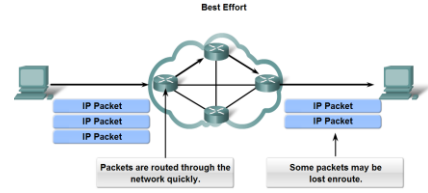
This process greatly reduces the overhead of IP.

Connectionless packet delivery may, however, result in packets arriving at the destination out of sequence.

If out-of-order or missing packets create problems for the application using the data, then upper layer services will have to resolve these issues.

Network Layer Protocols and Internet Protocol (IP)

Describe the implications for the use of the IP protocol as it is considered an unreliable protocol



As an unreliable Network layer protocol, IP does not guarantee that all sent packets will be received.

Other protocols manage the process of tracking packets and ensuring their delivery.

Unreliable Communication

The IP protocol does not burden the IP service with providing reliability. Compared to a reliable protocol, the IP header is smaller.

Transporting these smaller headers requires less overhead.

Less overhead means less delay in delivery. This characteristic is desirable for a Layer 3 protocol.

The mission of Layer 3 is to transport the packets between the hosts while placing as little burden on the network as possible.

Layer 3 is not concerned with or even aware of the type of communication contained inside of a packet.

This responsibility is the role of the upper layers as required.

The upper layers can decide if the communication between services needs reliability and if this communication can tolerate the overhead reliability requires.

Unreliable Communication

Unreliable means simply that IP does not have the capability to manage, and recover from, undelivered or corrupt packets.

Since protocols at other layers can manage reliability, IP is allowed to function very efficiently at the Network layer.

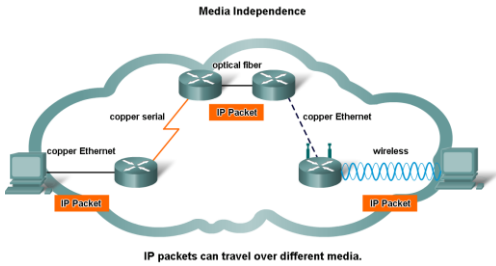
If we included reliability overhead in our Layer 3 protocol, then communications that do not require connections or reliability would be burdened with the bandwidth consumption and delay produced by this overhead.

In the TCP/IP suite, the Transport layer can choose either TCP or UDP, based on the needs of the communication.

As with all layer isolation provided by network models, leaving the reliability decision to the Transport layer makes IP more adaptable and accommodating for different types of communication.

Network Layer Protocols and Internet Protocol (IP)

Describe the implications for the use of the IP as it is media independent



Media Independant

The Network layer is also not burdened with the characteristics of the media on which packets will be transported. IPv4 and IPv6 operate independently of the media that carry the data at lower layers of the protocol stack.

As shown in the figure, any individual IP packet can be communicated electrically over cable, as optical signals over fiber, or wirelessly as radio signals.

It is the responsibility of the OSI Data Link layer to take an IP packet and prepare it for transmission over the communications medium. This means that the transport of IP packets is not limited to any particular medium.

MTU – Maximum Transmission Unit

There is, however, one major characteristic of the media that the Network layer considers: the maximum size of PDU that each medium can transport.

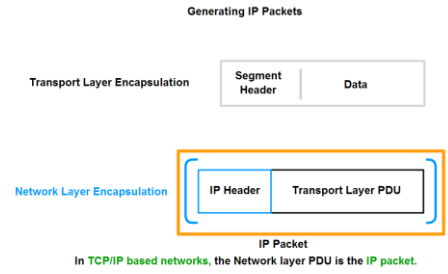
This characteristic is referred to as the ***Maximum Transmission Unit*** (MTU). Part of the control communication between the Data Link layer and the Network layer is the establishment of a maximum size for the packet.

The Data Link layer passes the MTU upward to the Network layer. The Network layer then determines how large to create the packets.

If the router needs to split the packet up to fit a particular MTU size, then this is known as ***fragmentation***

Network Layer Protocols and Internet Protocol (IP)

Describe the role of framing in the Transport Layer and explain that segments are encapsulated as packets



Framing at Layer 3

The process of encapsulating data by layer enables the services at the different layers to develop and scale without affecting other layers.

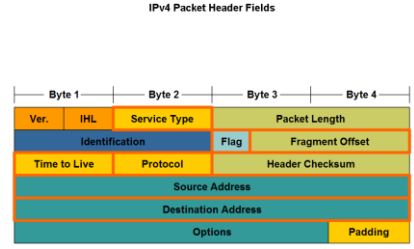
This means that Transport layer segments can be readily packaged by existing Network layer protocols, such as IPv4 and IPv6 or by any new protocol that might be developed in the future.

Routers can implement these different Network layer protocols to operate concurrently over a network to and from the same or different hosts.

The routing performed by these intermediary devices only considers the contents of the packet header that encapsulates the segment.

Network Layer Protocols and Internet Protocol (IP)

Identify the major header fields in the IPv4 protocol and describe each field's role in transporting packets



Header Fields

1. IP Source and Destination

2. TTL Value - is an 8-bit binary value that indicates the remaining "life" of the packet. The TTL value is decreased by at least one each time the packet is processed by a router (that is, each hop). When the value becomes zero, the router discards or drops the packet and it is removed from the network data flow

3. Protocol - This 8-bit binary value indicates the data payload type that the packet is carrying. The Protocol field enables the Network layer to pass the data to the appropriate upper-layer protocol e.g. 01 ICMP

4. Type of Service - contains an 8-bit binary value that is used to determine the priority of each packet. This value enables a Quality-of-Service (QoS) mechanism to be applied to high priority packets, such as those carrying telephony voice data.

Header Fields

5. Fragment offset - When fragmentation occurs, the IPv4 packet uses the Fragment Offset field and the MF flag in the IP header to reconstruct the packet when it arrives at the destination host. The fragment offset field identifies the order in which to place the packet fragment in the reconstruction.

6. The More Fragments (MF) flag is a single bit in the Flag field used with the Fragment Offset for the fragmentation and reconstruction of packets i.e. When MF value is set to 1 then expect more fragments, when set to 0 there are no more fragments to follow

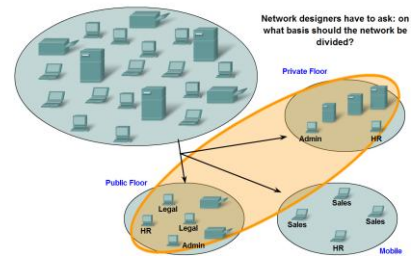
7. Don't Fragment Flag (DF) - a single bit in the Flag field that indicates that fragmentation of the packet is not allowed. If the Don't Fragment flag bit is set, then fragmentation of this packet is NOT permitted.

Other IPv4 Header Fields

1. **Version** - Contains the IP version number (4).
2. **Header Length (IHL)** - Specifies the size of the packet header.
3. **Packet Length** - This field gives the entire packet size, including header and data, in bytes.
4. **Identification** - This field is primarily used for uniquely identifying fragments of an original IP packet.
5. **Header Checksum** - The checksum field is used for error checking the packet header.
6. **Options** - There is provision for additional fields in the IPv4 header to provide other services but these are rarely used.

Grouping Devices into Networks and Hierarchical Addressing

List several different reasons for grouping devices into sub-networks and define several terms used to identify the sub-networks



Dividing Networks

Rather than having all hosts everywhere connected to one vast global network, it is more practical and manageable to group hosts into specific networks.

To alleviate these issues, the large network was separated into smaller networks that were interconnected.

These smaller networks are often called subnetworks or subnets.

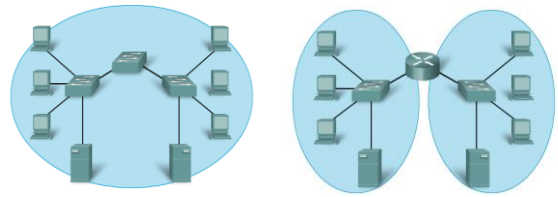
Network and subnet are terms often used interchangeably to refer to any network system made possible by the shared common communication protocols of the TCP/IP model.

Networks can be grouped based on factors that include:

1. Geographic location
2. Purpose
3. Ownership

Grouping Devices into Networks and Hierarchical Addressing

List several ways in which dividing a large network can increase network performance



Dividing Networks

As networks grow larger they present problems that can be at least partially alleviated by dividing the network into smaller interconnected networks.

Common issues with large networks are:

1. Performance degradation
2. Security issues
3. Address Management

Improving Performance

Large numbers of hosts connected to a single network can produce volumes of data traffic that may stretch, if not overwhelm, network resources such as bandwidth and routing capability. Dividing large networks so that hosts who need to communicate are grouped together reduces the traffic across the internetworks.

Broadcast Domains

A broadcast is a message sent from one host to all other hosts on the network.

Typically, a host initiates a broadcast when information about another unknown host is required.

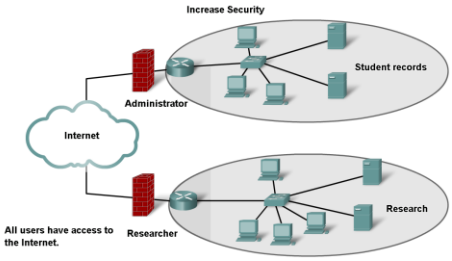
However, large numbers of hosts generate large numbers of broadcasts that consume network bandwidth.

And because every other host has to process the broadcast packet it receives, the other productive functions that a host is performing are also interrupted or degraded.

Managing the size of broadcast domains by dividing a network into subnets ensures that network and host performances are not degraded to unacceptable levels.

Grouping Devices into Networks and Hierarchical Addressing

List several ways in which dividing a large network can increase network security



Dividing the Network - Security

Dividing networks based on ownership means that access to and from resources outside each network can be prohibited, allowed, or monitored.

Internetwork access within a company or organization can be similarly secured.

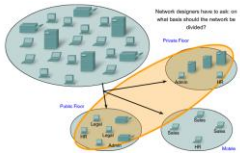
For example, a college network can be divided into administrative, research, and student subnetworks.

Dividing a network based on user access is a means to secure communications and data from unauthorized access by users both within the organization and outside it.

Security between networks is implemented in an intermediary device (a router or firewall appliance) at the perimeter of the network

Dividing the Network

Ownership



Subnets and Subnetworks

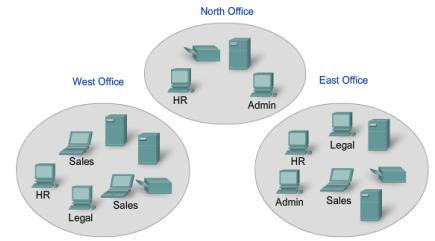
To alleviate issues, the large network was separated into smaller networks that were interconnected.

These smaller networks are often called subnetworks or subnets.

Networks can be grouped based on factors that include:

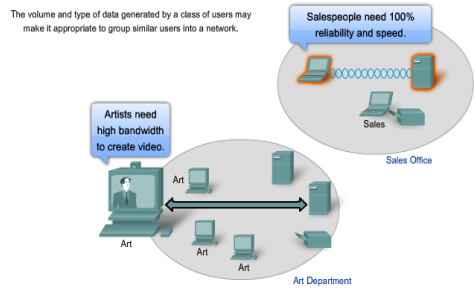
1. Geographic location
2. Purpose
3. Ownership

Geographic

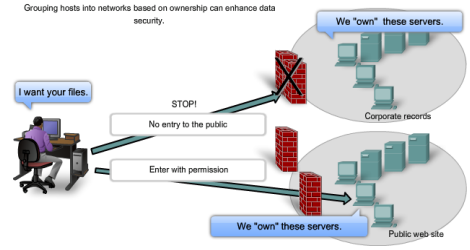


The simple fact of wiring together the physical network can make geographic location a logical place to start when segmenting a network.

Purpose

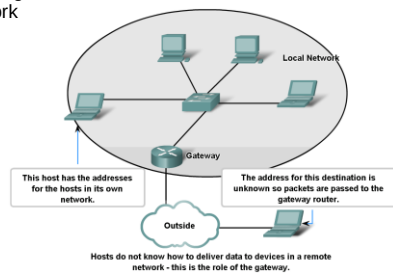


Ownership



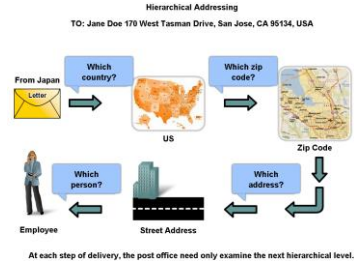
Grouping Devices into Networks and Hierarchical Addressing

Explain the communication problems that emerge when very large numbers of devices are included in one large network



Grouping Devices into Networks and Hierarchical Addressing

Describe how hierarchical addressing solves the problem of devices communicating across networks of networks



Hierarchical Addresses

To be able to divide networks, we need hierarchical addressing.

A hierarchical address uniquely identifies each host. It also has levels that assist in forwarding packets across internetworks, which enables a network to be divided based on those levels.

To support data communications between networks over internetworks, Network layer addressing schemes are hierarchical.

Layer 3 addresses supply the network portion of the address.

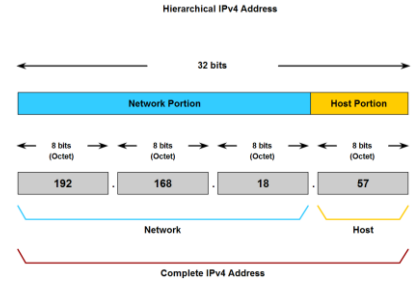
Routers forward packets between networks by referring only to the part of the Network layer address that is required to direct the packet toward the destination network.

By the time the packet arrives at the destination host network, the whole destination address of the host will have been used to deliver the packet.

Using a hierarchical addressing scheme means that the higher levels of the address (similar to the country in the postal address) can be retained, with the middle level denoting the network addresses (state or city) and the lower level the individual hosts.

Grouping Devices into Networks and Hierarchical Addressing

Describe the purpose of further subdividing networks into smaller networks



32-Bit Addressing

The logical 32-bit IPv4 address is hierarchical and is made up of two parts.

The first part identifies the network and the second part identifies a host on that network. Both parts are required for a complete IP address.

For convenience IPv4 addresses are divided in four groups of eight bits (octets). Each octet is converted to its decimal value and the complete address written as the four decimal values separated by a dot (period).

For example - 192.168.18.57

This is hierarchical addressing because the network portion indicates the network on which each unique host address is located.

Routers only need to know how to reach each network, rather than needing to know the location of each individual host.

Prefix Length

The number of bits of an address used as the network portion is called the prefix length.

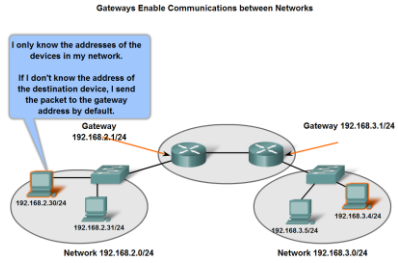
For example if a network uses 24 bits to express the network portion of an address the prefix is said to be /24. In the devices in an IPv4 network, a separate 32-bit number called a subnet mask indicates the prefix.

Extending the prefix length or subnet mask enables the creation of these subnetworks.

In this way network administrators have the flexibility to divide networks to meet different needs, such as location, managing network performance, and security, while ensuring each host has a unique address.

Fundamentals of Routes, Next Hop Addresses and Packet Forwarding

Describe the role of an intermediary gateway device in allowing devices to communicate across sub-divided networks



Intermediary Device

When a host needs to communicate with another network, an intermediary device, or router, acts as a gateway to the other network.

As a part of its configuration, a host has a default gateway address defined.

As shown in the figure, this gateway address is the address of a router interface that is connected to the same network as the host.

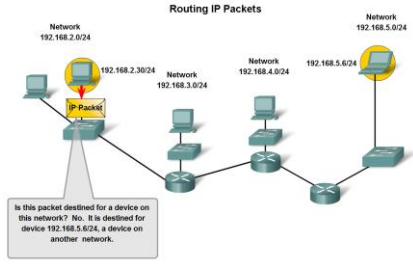
To communicate with a device on another network, a host uses the address of this gateway, or default gateway, to forward a packet outside the local network.

The router also needs a route that defines where to forward the packet next.

This is called the next-hop address. If a route is available to the router, the router will forward the packet to the next-hop router that offers a path to the destination network.

Fundamentals of Routes, Next Hop Addresses and Packet Forwarding

Trace the steps of an IP packet as it traverses unchanged via routers from sub network to sub-network



Routing Packets

If the destination host and source host are not in the same network, the packet may be carrying a Transport layer PDU across many networks and through many routers.

As it does, the information contained within is not altered by any routers when forwarding decisions are made.

At each hop, the forwarding decisions are based on the information in the IP packet header.

The packet with its Network Layer encapsulation also is basically intact throughout the complete process, from the source host to the destination host.

If communication is between hosts in different networks, the local network delivers the packet from the source to its gateway router

How it Works

The router examines the network portion of the packet destination address and forwards the packet to the appropriate interface.

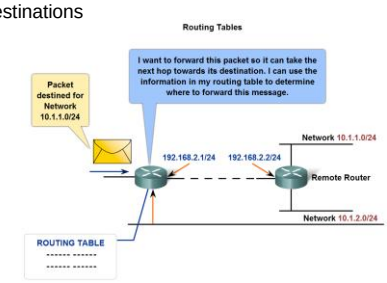
If the destination network is directly connected to this router, the packet is forwarded directly to that host. If the destination network is not directly connected, the packet is forwarded on to a second router that is the next-hop router.

The packet forwarding then becomes the responsibility of this second router.

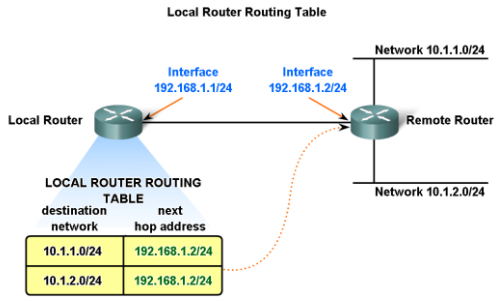
Many routers or hops along the way may process the packet before reaching the destination.

Fundamentals of Routes, Next Hop Addresses and Packet Forwarding

Describe the role of a gateway and the use of a simple route table in directing packets toward their ultimate destinations



Fundamentals of Routes, Next Hop Addresses and Packet Forwarding



Routing

No packet can be forwarded without a route.

Whether the packet is originating in a host or being forwarded by an intermediary device, the device must have a route to identify where to forward the packet.

A host must either forward a packet to the host on the local network or to the gateway, as appropriate.

To forward the packets, the host must have routes that represent these destinations.

A router makes a forwarding decision for each packet that arrives at the gateway interface.

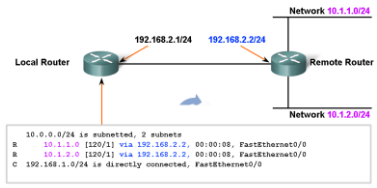
This forwarding process is referred to as routing.

To forward a packet to a destination network, the router requires a route to that network. If a route to a destination network does not exist, the packet cannot be forwarded.

Fundamentals of Routes, Next Hop Addresses and Packet Forwarding

Describe the purpose and use of the destination network in a route

Confirming the Gateway and Route



This is the routing table output of Local Router when the "show ip route" is issued.

The next hop for networks 10.1.1.0/24 and 10.1.2.0/24 from Local Router is 192.168.2.2.

Routing Table

A route for packets for remote destinations is added using the default gateway address as the next hop. Although it is not usually done, a host can also have routes manually added through configurations.

Like end devices, routers also add routes for the connected networks to their routing table.

When a router interface is configured with an IP address and subnet mask, the interface becomes part of that network.

The routing table now includes that network as a directly connected network. All other routes, however, must be configured or acquired via a routing protocol.

To forward a packet the router must know where to send it. This information is available as routes in a routing table.

Routing Table Features

Routes in a routing table have three main features:

1. Destination network
2. Next-hop
3. Metric - Indicates how many internetwork hops (routers) have been traversed in the trip to the destination. This value is between 1 and 15 for a valid route, or 16 for an unreachable route

The router matches the destination address in the packet header with the destination network of a route in the routing table and forwards the packet to the next-hop router specified by that route.

If there are two or more possible routes to the same destination, the metric is used to decide which route appears on the routing table.

Fundamentals of Routes, Next Hop Addresses and Packet Forwarding

Describe the purpose and use of the next hop in a route

Routing Table Output with Next Hops

Next Hop Routing

This is a critical concept in how IP works: routing is done on a step-by-step basis, one hop at a time.

When we decide to send a datagram to a device on a distant network, we don't know the exact path that the datagram will take; we only have enough information to send it to the correct router to which we are attached.

That router, in turn, looks at the IP address of the destination and decides where the datagram should next "hop" to.

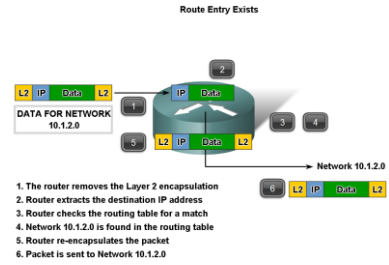
This process continues until the datagram reaches the destination host's network, when it is delivered.

Next-hop routing may seem at first like a strange way of communicating datagrams over an internetwork. In fact, it is part of what makes IP so powerful.

On each step of the journey to any other host, a router only needs to know where the next step for the datagram is. Without this concept, each device and router would need to know what path to take to every other host on the internet, which would be quite impractical.

Fundamentals of Routes, Next Hop Addresses and Packet Forwarding

Trace the steps of several IP packets as they are routed through several gateways from devices on one sub network to devices on other sub networks



Default Routes

If the routing table does not contain a more specific route entry for an arriving packet, the packet is forwarded to the interface indicated by a default route, if one exists.

At this interface, the packet is encapsulated by the Layer 2 protocol and sent to the next-hop router.

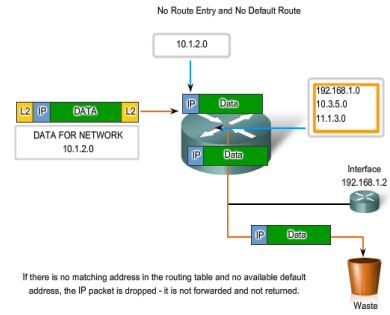
The default route is also known as the Gateway of Last Resort.

Default routes are important because the gateway router is not likely to have a route to every possible network on the Internet.

If the packet is forwarded using a default route, it should eventually arrive at a router that has a specific route to the destination network.

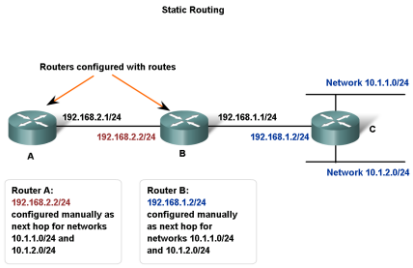
This router may be the router to which this network is attached. In this case, this router will forward the packet over the local network to the destination host.

No Route Entry?



Fundamentals of Routes, Next Hop Addresses and Packet Forwarding

Describe the purpose of routing protocols and the need for both static and dynamic routes



Static Routes

Routes to remote networks with the associated next hops can be manually configured on the router. This is known as static routing.

A default route can also be statically configured. (Usually depicted as 0.0.0.0 0.0.0.0)

If the router is connected to a number of other routers, knowledge of the internetworking structure is required.

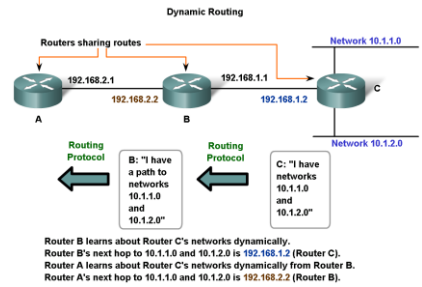
To ensure that the packets are routed to use the best possible next hops, each known destination network needs to either have a route or a default route configured.

Because packets are forwarded at every hop, every router must be configured with static routes to next hops that reflect its location in the internetwork.

Can be more hassle as any changes will have to be manually changed by the administrator

Fundamentals of Routes, Next Hop Addresses and Packet Forwarding

Explain how routes are manually configured to build routing table



Dynamic Routing

Routing protocols are the set of rules by which routers dynamically share their routing information.

As routers become aware of changes to the networks for which they act as the gateway, or changes to links between routers, this information is passed on to other routers.

When a router receives information about new or changed routes, it updates its own routing table and, in turn, passes the information to other routers.

In this way, all routers have accurate routing tables that are updated dynamically and can learn about routes to remote networks that are many hops way.

An example of router sharing routes is shown in the figure.

Common routing protocols are:

1. ***Routing Information Protocol (RIP)***
2. ***Enhanced Interior Gateway Routing Protocol (EIGRP)***
3. ***Open Shortest Path First (OSPF)***

Disadvantages

Although routing protocols provide routers with up-to-date routing tables, there are costs.

First, the exchange of route information adds overhead that consumes network bandwidth.

This overhead can be an issue, particularly for low bandwidth links between routers.

Second, the route information that a router receives is processed extensively by protocols such as EIGRP and OSPF to make routing table entries.

This means that routers employing these protocols must have sufficient processing capacity to both implement the protocol's algorithms and to perform timely packet routing and forwarding.

Hybrid Routing

Static routing does not produce any network overhead and places entries directly into the routing table; no processing is required by the router.

The cost for static routing is administrative - the manual configuration and maintenance of the routing table to ensure efficient and effective routing.

In many internetworks, a combination of static, dynamic, and default routes are used to provide the necessary routes.

Fundamentals of Routes, Next Hop Addresses and Packet Forwarding

Explain the role of routing protocols in building the routing table

Summary

In this chapter, you learned to:

- Identify the role of the Network layer as it describes communication from one end device to another end device.
- Examine the most common Network layer protocol, Internet Protocol (IP), and its features for providing connectionless and best-effort service.
- Describe the principles used to guide the division, or grouping, of devices into networks.
- Explain the purpose of the hierarchical addressing of devices and how this allows communication between networks.
- Describe the fundamentals of routes, next-hop addresses, and packet forwarding to a destination network.