Home > My courses > Network Defense and Remote Access Configuration > 03 [Enter Module Title Here] > Lesson Proper for Week 3

Lesson Proper for Week 3

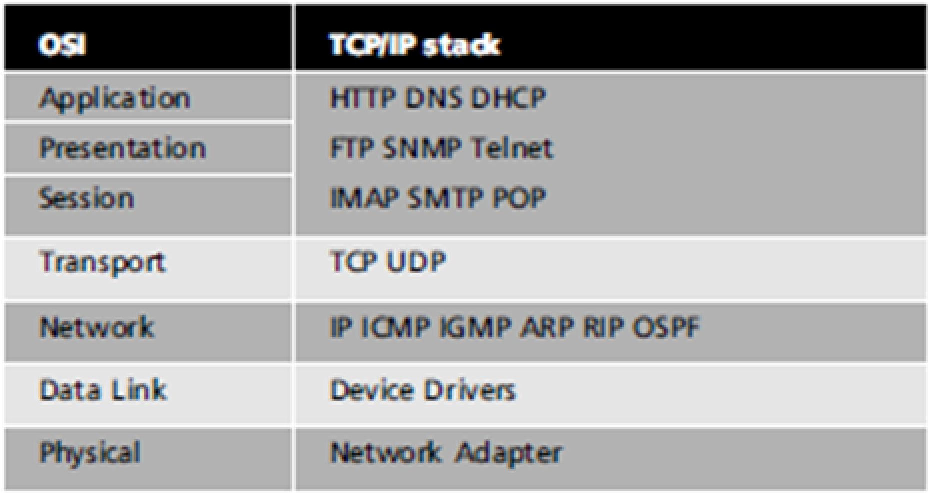
TCP/IP I

THE OSI MODEL AND TCP/IP PROTOCOLS

Transmission Control Protocol/Internet Protocol (TCP/IP) is a suite of many protocols for transmitting information from point to point on a network. (This suite of protocols is often called a stack.) You may already know TCP/IP, but it never hurts to brush up on your knowledge. Given the dynamic nature of information technology, you can forget even simple details, so this section gives you a quick refresher on TCP/IP basics, such as the Open Systems Interconnection (OSI) model, IP addressing, and subnetting.

The OSI Model

You are probably familiar with the OSI reference model of network communications, which divides the communication functions used by two hosts into seven separate layers. TCP/IP has its own stack of protocols that correspond roughly to these layers. Table 2-1 compares the two models.



OSI	TCP/IP stack
Application	HTTP DNS DHCP
Presentation	FTP SNMP Telnet
Session	IMAP SMTP POP
Transport	TCP UDP
Network	IP ICMP IGMP ARP RIP OSPF
Data Link	Device Drivers
Physical	Network Adapter

Table 2-1 The OSI model and the subprotocols of the TCP/IP stack

You should be familiar with most of these protocols and their functions. The following list provides a brief review of some protocols; more detailed discussions of TCP, UDP, IP, ICMP, IGMP, and ARP are included later in this chapter. If you need a more detailed refresher on the TCP/IP stack, the OSI model, and the major protocols operating at different layers, perform an Internet search on "TCP/IP and the OSI model." Dozens of helpful sites, such as www.tcpipguide.com/free/index.htm, are available for every level of knowledge.

Note that the top three layers of the OSI model—Application, Presentation, and Session—are considered equivalent to the top layer of the TCP/IP stack. The TCP/IP subprotocols listed in this layer are services that support a number of network functions:

- HTTP (Hypertext Transfer Protocol) is responsible for the delivery of Web documents formatted in HTML (Hypertext Markup Language) and other similar languages.
- DNS (Domain Name System) is responsible for the resolution of fully qualified domain names (for example, support.microsoft.com) to IP addresses, as well as resolution of IP addresses to fully qualified domain names.
- DHCP (Dynamic Host Configuration Protocol) is responsible for automatic assignment of IP addresses and other configuration data to client systems.
- FTP (File Transport Protocol) provides efficient delivery of files from one system to another.
- SNMP (Simple Network Management Protocol) monitors various parameters on network devices like switches and servers.
- Telnet is a terminal emulation service that allows users to run commands on a remote system.
- IMAP, SMTP, and POP are used in e-mail communications. Internet Message Access Protocol is used for downloading e-mail, Simple Mail Transfer Protocol is used for sending e-mail, and Post Office Protocol, like IMAP, downloads e-mail. Unlike IMAP, however, POP does not allow the user to determine which messages are removed from the e-mail server.

The TCP/IP routing protocols RIP and OSPF are processed at the Network layer of the OSI model. These protocols allow routers to share their routing tables with each other. (Routing is covered in detail in Chapter 4.)

TCP/IP Addressing

IP addresses are one of the methods used to identify computers. These addresses are processed at the Network layer of the OSI model. The type of IP addresses most commonly in use conform to **Internet Protocol version 4 (IPv4)**, which specifies addresses with 32 bits of data. Each 32-bit address is divided into four groups called octets; each octet contains 8 bits of data. In binary, an IP address looks like this:
10000000.00100110.00101100.11100010

While binary numbers are no problem for computers, this notation is difficult for humans to manage; therefore, IP addresses are usually converted to dotted decimal notation, such as 192.168.10.1. An IP address consists of two main parts:

- The **network identifier**, which is the part of an IP address shared among computers in a network segment
- The **host identifier**, which is unique to each computer on the network segment

These two identifiers are defined by another dotted decimal value called the **subnet mask**. This value indicates which part of the IP address is the network identifier and which part is the host identifier. You learn more about subnet masks in the “Subnetting” section later in this chapter.

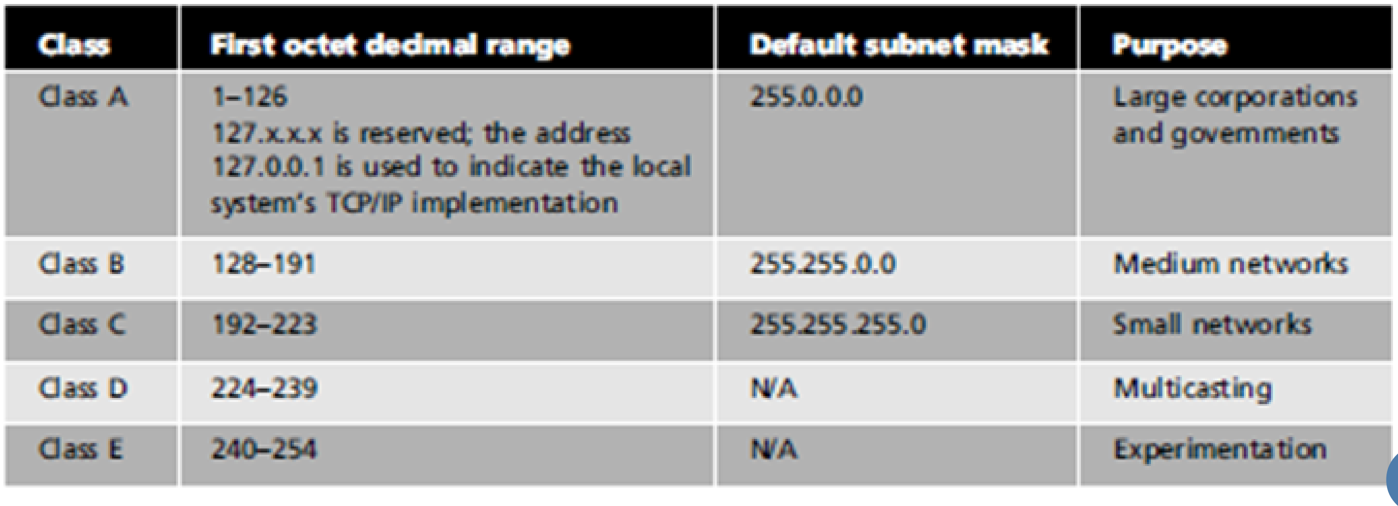
One way attackers can gain access to your network is by determining the IP addresses of computers. After they have an address, they can attempt to take over the computer and use it to launch attacks on other computers in the network or access network resources. Therefore, a fundamental requirement of network security is to understand IP addresses and other network addresses so that you can conceal or change them to deter attackers.

IP addresses are valuable commodities. If attackers can find a computer’s IP address, they can run a port scan to look for open ports they can exploit. By hiding IP addresses, you can prevent certain attacks. To hide the addresses of computers on your network, you can use **Network Address Translation (NAT)** to translate your private network’s internal addresses into the address of the NAT server’s external interface connected to the Internet. A private network’s internal addresses are not routable on the Internet.

Security is not the only reason for using NAT. The Internet has grown more quickly than expected by the creators of the IPv4 32-bit addressing scheme. Today, IP addresses are in short supply, so Internet Protocol version 6 (IPv6) is being implemented.

Address Classes

IPv4 addresses are separated into address categories called classes. An IP address class is determined by the number of its networks compared to the number of its hosts. For example, a Class A address uses 8 bits for the network portion of the address and 24 bits for the host portion. The class divisions are shown in Table 2-2.



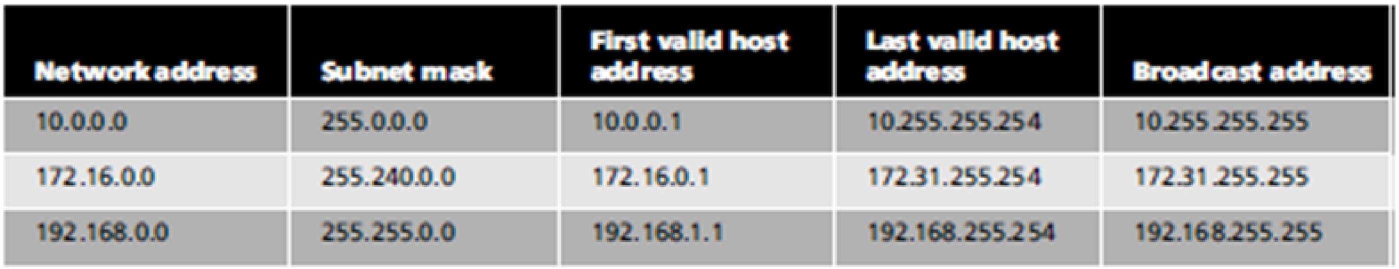
Class	First octet decimal range	Default subnet mask	Purpose
Class A	1–126 127.x.x.x is reserved; the address 127.0.0.1 is used to indicate the local system’s TCP/IP implementation	255.0.0.0	Large corporations and governments
Class B	128–191	255.255.0.0	Medium networks
Class C	192–223	255.255.255.0	Small networks
Class D	224–239	N/A	Multicasting
Class E	240–254	N/A	Experimentation

Table 2-2 IP address classes

Private IP Address Ranges

In addition to public address ranges, which are used to move messages from one network to another, protocol designers recognized the need for a private addressing system that organizations could use to build internal infrastructures. To obtain a public IP address, individuals and organizations must register and pay a fee for each address. Addresses with large quantities of hosts carry a higher price tag than those with fewer host addresses. The private addressing scheme eliminated the need to purchase addresses for every group of machines. However, the free address space carries a price. Private addresses are not routable over the Internet. RFC (Request for Comments) 1918 defined ranges of reserved private IP addresses that organizations can use on their internal networks. No Internet host can directly access an organization's computers as long as they have only private IP addresses. Table 2-3 lists the private IP address ranges.

RFCs are the documents that create standards for Internet technology. You should become familiar with RFCs so that you can keep up with changes as they occur. You can read RFC 1918 at http://tools.ietf.org/html/rfc1918.



Network address	Subnet mask	First valid host address	Last valid host address	Broadcast address
10.0.0.0	255.0.0.0	10.0.0.1	10.255.255.254	10.255.255.255
172.16.0.0	255.240.0.0	172.16.0.1	172.31.255.254	172.31.255.255
192.168.0.0	255.255.0.0	192.168.1.1	192.168.255.254	192.168.255.255

Table 2-3 Private IP address ranges

Subnetting

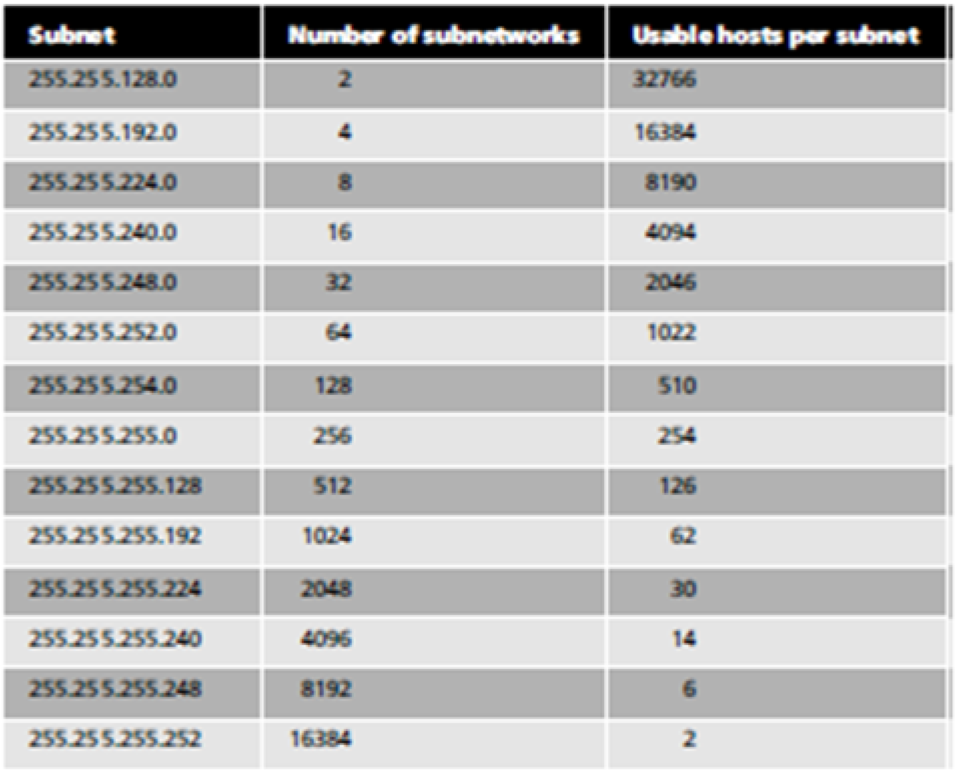
As mentioned, an IP address and its subnet mask identify both the network and the host. Address classes already have network identification octets in the subnet mask set by default; Class A has the first octet set, Class B the first two, and Class C the first three (see Table 2-2). The remainder of the address is available for extending the network identifier portion of the subnet mask. For example, a default Class B address has 16 bits available for the host portion of the address. This means that a single Class B network has more than 65,000 host addresses! However, many organizations use some of the host bits to identify the network; this approach creates several smaller subnetworks that are more flexible and easier to manage than one large network.

Subnetting is used to segment internal networks logically, as described previously. It can also be used for the following purposes:

- Mirroring the organization's physical layout
- Mirroring the organization's administrative structure
- Planning for future growth
- Reducing and controlling network traffic
- Increasing network security

When administrators create subnetworks that mirror the organization's structure or physical layout, managing security, access needs, and auditing becomes easier. This concept is similar to creating sites and domains. Trying to manage many different user groups gets complicated. If all users with similar security and access needs are grouped into a single subnet, the entire group can be managed instead of managing each user separately. Subnets are used to make network management easier and to optimize security, performance, and access.

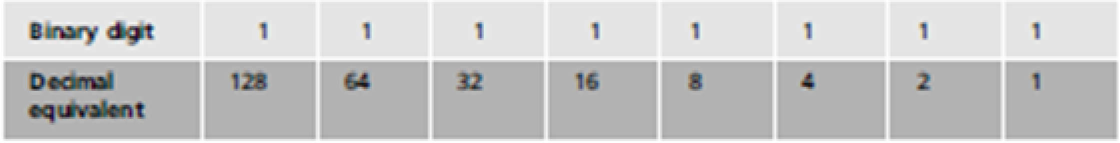
When administrators create subnets, they borrow bits from the host portion of the IP address to make a set of subnetworks. The number of borrowed bits determines how many subnets and hosts are available. An administrator can use up to 14 bits for subnetting a Class B network. (Two bits must be available for hosts.) When you subnet, you lose some addresses that would have been available for hosts, but a network of 65,000 hosts would be unwieldy to manage, and performance would suffer with so much traffic on a single network segment. Table 2-4 shows how subnetting is used on Class B networks.



Subnet	Number of subnetworks	Usable hosts per subnet
255.255.128.0	2	32766
255.255.192.0	4	16384
255.255.224.0	8	8190
255.255.240.0	16	4094
255.255.248.0	32	2046
255.255.252.0	64	1022
255.255.254.0	128	510
255.255.255.0	256	254
255.255.255.128	512	126
255.255.255.192	1024	62
255.255.255.224	2048	30
255.255.255.240	4096	14
255.255.255.248	8192	6
255.255.255.252	16384	2

Table 2-4 Class B subnetting

Although you should already have a good working knowledge of subnetting, a brief refresher is useful. You might find it helpful to remember how the binary numbering system stacks up to the decimal system in IP addressing. Table 2-5 shows the decimal equivalents of binary place values.



Binary digit	1	1	1	1	1	1	1	1
Decimal equivalent	128	64	32	16	8	4	2	1

Table 2-5 Binary-to-decimal values

Now that you remember what decimal value is represented by each binary digit in an IP octet, you can review subnetting. First, you select the mask that meets your needs, and then you assign the mask to your network. To do this, you must find the usable IP address ranges for the network address, the valid host address range, and the broadcast address. Converting the last masking octet to binary performs this task most easily. The binary place value of the last masking digit is the block size. (Block size refers to the maximum number of host addresses plus the subnetwork and broadcast address in a subnet.) Subnetting a Class C address goes like this:

Class C address: 199.1.10.0 (network address)

Default mask: 255.255.255.0

Selected mask: 255.255.255.224

Mask converted to binary: 11111111.11111111.11111111.11100000

Notice that the last masked digit occupies the binary place value of 32 (which is the block size). Starting with the network address, increment by 32 until you reach the mask's number (224). It looks like this:

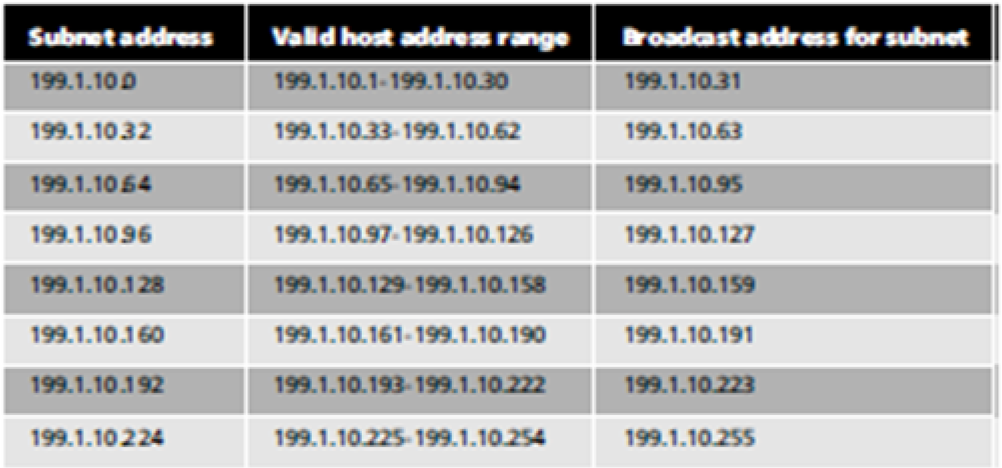
- 0 (00000000)
- 32 (00100000)
- 64 (01000000)
- 96 (01100000)
- 128 (10000000)
- 160 (10100000)
- 192 (11000000)
- 224 (11100000)

If you first learned to subnet some years ago, you might have learned that the subnetwork identifier cannot be all binary zeros or all binary ones. This was true when Routing Information Protocol version 1 (RIPv1) was in use. With subsequent routing protocols such as RIPv2 and OSPF (Open Shortest Path First), all zeros and all ones are permitted in the subnet identifier.

Table 2-6 shows the subnetwork addresses, host address ranges, and broadcast addresses for this example.

When looking at the chart, you might notice that the host address range includes only 30 valid hosts. What happened to the other two hosts? When you calculate a host range, or block size, you include one address for the network address and one for the broadcast address. These two addresses cannot be assigned to hosts. Therefore, you can use the following formula to calculate the number of valid hosts:

2x – 2 = Number of valid hosts per subnet (the exponent x is the number of bits in the host identifier)



Subnet address	Valid host address range	Broadcast address for subnet
199.1.10.0	199.1.10.1-199.1.10.30	199.1.10.31
199.1.10.32	199.1.10.33-199.1.10.62	199.1.10.63
199.1.10.64	199.1.10.65-199.1.10.94	199.1.10.95
199.1.10.96	199.1.10.97-199.1.10.126	199.1.10.127
199.1.10.128	199.1.10.129-199.1.10.158	199.1.10.159
199.1.10.160	199.1.10.161-199.1.10.190	199.1.10.191
199.1.10.192	199.1.10.193-199.1.10.222	199.1.10.223
199.1.10.224	199.1.10.225-199.1.10.254	199.1.10.255

Table 2-6 Subnetting example

Variable Length Subnet Masking

Networks that do not have a large number of available IP addresses can use **variable length subnet masking (VLSM)**, which involves applying masks of varying sizes to the same network. If an organization has a limited number of IP addresses and subnets of varying lengths, VLSM can help it use address space more efficiently. VLSM is a means of allocating IP addressing according to the network's needs. This allocation method creates subnets within subnets and multiple divisions of an IP network. VLSM is often used to secure stub networks—"dead end" networks that have only one connection to any other network. VLSM is also used to secure serial lines, which are connections between remote networks that require only two IP addresses. In these cases, VLSM makes the subnets only as large as needed.

Classless Interdomain Routing

Classless Interdomain Routing (CIDR) is an address notation scheme that specifies the number of masked bits in an IP address/subnet mask combination. Instead of using standard notation for subnet masks, with CIDR you can simply list the number of masked binary bits. The subnet mask 255.255.255.224, for example, has a total of 27 masked bits (eight in each of the first three octets and three in the last octet). In CIDR notation, you would write the network address 192.168.6.0 with a subnet mask of 255.255.255.224 as 192.168.6.0/27. CIDR overcomes the limitations of the default subnet masks of 8, 16, and 24 bits for Classes A, B, and C (classful addressing) so that unused addresses do not go to waste.

If you use subnet masks to segment network traffic into a series of smaller subnetworks, plan in advance how you will allocate nodes to each segment and assign subnet masks to those segments. Your planning might include network growth projections for the next two to five years so that you will not have to set up different subnet designations with each future network change.

Supernetting, also known as summarization, is used to summarize multiple routing table entries into one entry. In addition, classless routing is used to exchange subnet mask information between routers in routing updates. Classless routing allows VLSM and supernetting to work.

Unicasting, Multicasting, and Broadcasting

Each IP address class (Class A through Class D) is used with a different type of network. The address classes reflect the network's size and whether the packet is unicast or multicast. In a **unicast** transmission, one packet is sent from a server computer to each client computer that requests a file or an application, such as a streaming video presentation. If five clients request the video presentation, the server transmits the presentation separately to each client. In the same example, a **multicast** transmission means the server can treat all five clients as a group and send one transmission that reaches all of them. Multicasts can be used to reduce network traffic when transmitting bandwidth-intensive applications or files to multiple hosts. Instead of sending one to each host separately, the files or applications can be sent to all recipients at once.

A third type of network communication called a **broadcast** sends a communication to all points on a specific network. (Routers are usually configured so that they do not forward broadcasts to other networks.) There are two types of broadcasts:

- Flooded broadcasts are sent to any subnet. Routers do not forward the broadcasts because they are considered local. These broadcasts use the address 255.255.255.255.
- Directed broadcasts are sent to a specific subnet. Routers forward directed broadcasts using the broadcast address for the intended subnet.

EXAMINING INTERNET PROTOCOL VERSION 4 (IPV4)

TCP/IP is packet-based; it gives computers a fairly simple framework for transmitting information in small chunks called packets. Unfortunately, TCP/IP packets give attackers another way to gain entry into a network. Attackers can intercept packets and falsify the information in them or manipulate the packets in a way that makes it impossible for receiving servers to respond, which then disables those servers and opens the network to attack.

IP Datagrams

The portion of the packet that IP is responsible for routing through networks is called an **IP datagram**. This portion of the packet is processed at the Network layer of the OSI model. Each complete message is usually separated into multiple datagrams. Each datagram contains information about the source and destination IP addresses, a variety of control settings, and the actual data message that the computers are exchanging.

Each IP datagram is divided into different sections. The primary subdivisions are the header and the data, as described in the following sections. Some packets have another segmented section at the end called a footer (or "trailer"), which contains data that indicates the end of the packet. An error-checking algorithm called a Cyclic Redundancy Check (CRC) might also be added in the footer.

◀ Preliminary Activity for Week 3

Jump to... ⌄

Analysis, Application, and Exploration for Week 3 ▶

Navigation

- Home
- Dashboard
  - Site pages
  - My courses
    - Capstone Project 2
    - Network Defense and Remote Access Configuration
      - Participants
      - General
      - 01 [Enter Module Title Here]
      - 02 [Enter Module Title Here]
      - 03 [Enter Module Title Here]
        - Preliminary Activity for Week 3
        - **Lesson Proper for Week 3**
        - Analysis, Application, and Exploration for Week 3
        - Generalization for Week 3
        - Evaluation for Week 3
        - Assignment for Week 3
      - 04 [Enter Module Title Here]
      - 05 [Enter Module Title Here]
    - OJT/Practicum 2
    - Seminars and Tours
  - Courses

Fair Warning

NOTICE: Please be reminded that it has come to the attention of the Publishing Team of eLearning Commons that learning materials published and intended for ***free use only by students and faculty members within the eLearning Commons network were UNLAWFULLY uploaded in other sites without due and proper permission***.

PROSECUTION: Under Philippine law (Republic Act No. 8293), copyright infringement is punishable by the following: Imprisonment of between 1 to 3 years and a fine of between 50,000 to 150,000 pesos for the first offense. Imprisonment of 3 years and 1 day to six years plus a fine of between 150,000 to 500,000 pesos for the second offense.

COURSE OF ACTION: Whoever has maliciously uploaded these concerned materials are hereby given an ultimatum to take it down within 24-hours. Beyond the 24-hour grace period, our Legal Department shall initiate the proceedings in coordination with the National Bureau of Investigation for IP Address tracking, account owner identification, and filing of cases for prosecution.

Activities

- Assignments
- Forums
- Quizzes
- Resources

Bestlink College of the Philippines
College Department

Powered byeLearning Commons