NETWORKING TECHNOLOGIES (20BHM513)

UNIT-IV

1. INTERNET PROTOCOL (IP)

The Internet Protocol (IP) is a protocol, or set of rules, for routing and addressing packets of data so that they can travel across networks and arrive at the correct destination. Data traversing the Internet is divided into smaller pieces, called packets. IP information is attached to each packet, and this information helps routers to send packets to the right place. Every device or domain that connects to the Internet is assigned an IP address, and as packets are directed to the IP address attached to them, data arrives where it is needed.

Once the packets arrive at their destination, they are handled differently depending on which transport protocol is used in combination with IP. The most common transport protocols are TCP and UDP.

2. IP ADDRESS

An IP address is a unique identifier assigned to a device or domain that connects to the Internet. Each IP address is a series of characters, such as '192.168.1.1'. Via DNS resolvers, which translate human-readable domain names into IP addresses, users are able to access websites without memorizing this complex series of characters. Each IP packet will contain both the IP address of the device or domain sending the packet and the IP address of the intended recipient, much like how both the destination address and the return address are included on a piece of mail.

Example: IPv4 vs. IPv6

The fourth version of IP (IPv4 for short) was introduced in 1983. However, just as there are only so many possible permutations for automobile license plate numbers and they have to be reformatted periodically, the supply of available IPv4 addresses has become depleted. IPv6 addresses have many more characters and thus more permutations; however, IPv6 is not yet completely adopted, and most domains and devices still have IPv4 addresses.

3. OSPF

Open Shortest Path First (OSPF) is a link-state routing protocol that is used to find the best path between the source and the destination router using its own Shortest Path First). OSPF is developed by Internet Engineering Task Force (IETF) as one of the Interior Gateway Protocol

(IGP), i.e, the protocol which aims at moving the packet within a large autonomous system or routing domain.

OSPF Terms

1. **Router Id –** It is the highest active IP address present on the router. First, the highest loopback address is considered. If no loopback is configured then the highest active IP address on the interface of the router is considered.
2. **Router priority –** It is an 8-bit value assigned to a router operating OSPF, used to elect DR and BDR in a broadcast network.
3. **Designated Router (DR) –** It is elected to minimize the number of adjacencies formed. DR distributes the LSAs to all the other routers. DR is elected in a broadcast network to which all the other routers share their DBD. In a broadcast network, the router requests for an update to DR, and DR will respond to that request with an update.
4. **Backup Designated Router (BDR) –** BDR is a backup to DR in a broadcast network. When DR goes down, BDR becomes DR and performs its functions.
5. **DR and BDR election –** DR and BDR election takes place in the broadcast network or multi-access network. Here are the criteria for the election:
    - The router having the highest router priority will be declared as DR.
    - If there is a tie in router priority then the highest router I'd be considered. First, the highest loopback address is considered. If no loopback is configured then the highest active IP address on the interface of the router is considered.

OSPF States

The device operating OSPF goes through certain states. These states are:

- **Down –** In this state, no hello packets have been received on the interface. **Note –** The Downstate doesn't mean that the interface is physically down. Here, it means that the OSPF adjacency process has not started yet.
- **INIT –** In this state, the hello packets have been received from the other router.
- **2WAY –** In the 2WAY state, both the routers have received the hello packets from other routers. Bidirectional connectivity has been established.
- **Note –** In between the 2WAY state and Exstart state, the DR and BDR election takes place.

- **Exstart –** In this state, NULL DBD are exchanged. In this state, the master and slave elections take place. The router having the higher router I'd become the master while the other becomes the slave. This election decides which router will send its DBD first
- **Exchange –** In this state, the actual DBDs are exchanged.
- **Loading –** In this state, LSR, LSU, and LSA (Link State Acknowledgement) are exchanged.

  Important – When a router receives DBD from other router, it compares its own DBD with the other router DBD. If the received DBD is more updated than its own DBD then the router will send LSR to the other router stating what links are needed. The other router replies with the LSU containing the updates that are needed. In return to this, the router replies with the Link State Acknowledgement.
- **Full –** In this state, synchronization of all.

4. BGP

Border Gateway Protocol (BGP) is used to Exchange routing information for the internet and is the protocol used between ISP which are different. The protocol can connect together any internetwork of autonomous system using an arbitrary topology. The only requirement is that each AS have at least one router that is able to run BGP and that is router connect to at least one other AS's BGP router. BGP's main function is to exchange network reach-ability information with other BGP systems. Border Gateway Protocol constructs an autonomous systems' graph based on the information exchanged between BGP routers.

Characteristics of Border Gateway Protocol (BGP):

- **Inter-Autonomous System Configuration:** The main role of BGP is to provide communication between two autonomous systems.
- BGP supports Next-Hop Paradigm.
- Coordination among multiple BGP speakers within the AS (Autonomous System).
- **Path Information:** BGP advertisement also include path information, along with the reachable destination and next destination pair.
- **Policy Support:** BGP can implement policies that can be configured by the administrator. **For ex: -** a router running BGP can be configured to distinguish between the routes that are known within the AS and that which are known from outside the AS.
- Runs Over TCP.
- BGP conserve network Bandwidth.

- BGP supports CIDR.
- BGP also supports Security.

Functionality of Border Gateway Protocol (BGP):

BGP peers performs 3 functions, which are given below.

1. The first function consist of initial peer acquisition and authentication. both the peers established a TCP connection and perform message exchange that guarantees both sides have agreed to communicate.
2. The second function mainly focus on sending negative or positive reach-ability information.
3. The third function verifies that the peers and the network connection between them are functioning correctly.

BGP Route Information Management Functions:

- **Route Storage:** Each BGP stores information about how to reach other networks.
- **Route Update:** In this task, Special techniques are used to determine when and how to use the information received from peers to properly update the routes.
- **Route Selection:** Each BGP uses the information in its route databases to select good routes to each network on the internet network.
- **Route advertisement:** Each BGP speaker regularly tells its peer what is known about various networks and methods to reach them.

5. WIRELESS TRANSACTION PROTOCOL

Transaction Layer contains Wireless Transaction Protocol (WTP). It runs on top of UDP (User Datagram Protocol) and is a part of TCP/IP and offers transaction support.

The wireless transaction protocol (WTP) is on top of either WDP or, if security is required, WTLS (WAP Forum, 2000d). WTP has been designed to run on very thin clients, such as mobile phones. WTP offers several advantages to higher layers, including an improved reliability over datagram services, improved efficiency over connection-oriented services, and support for transaction-oriented services such as web browsing. Class 0 provides unreliable message transfer without any result message. Classes 1 and 2 provide reliable message transfer, class 1 without, class 2 with, exactly one reliable result message (the typical request/response case).

WTP class 0

The WTP layer will transmit the user data (UD) transparently to its destination. The class type C indicates here class 0. Finally, the transaction handle H provides a simple index to uniquely identify the transaction and is an alias for the tuple (SA, SP, DA, DP), i.e., a socket pair, with only local significance.

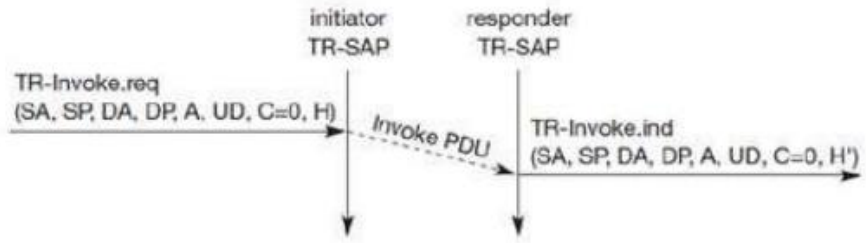


Fig 4.6 Basic Transaction , WTP Class 0

WTP class 1 Class 1 offers a reliable transaction service but without a result message. Again, the initiator sends an invoke PDU after a TR-Invoke.req from a higher layer. This time, class equals „1, and no user acknowledgement has been selected as shown in Figure. The responder signals the incoming invoke PDU via the TR-Invoke.ind primitive to the higher layer and acknowledges automatically without user intervention. The specification also allows the user on the responders' side to acknowledge, but this acknowledgement is not required. For the initiator the transaction ends with the reception of the acknowledgement. The responder keeps the transaction state for some time to be able to retransmit the acknowledgement if it receives the same invoke PDU again indicating a loss of the acknowledgement.

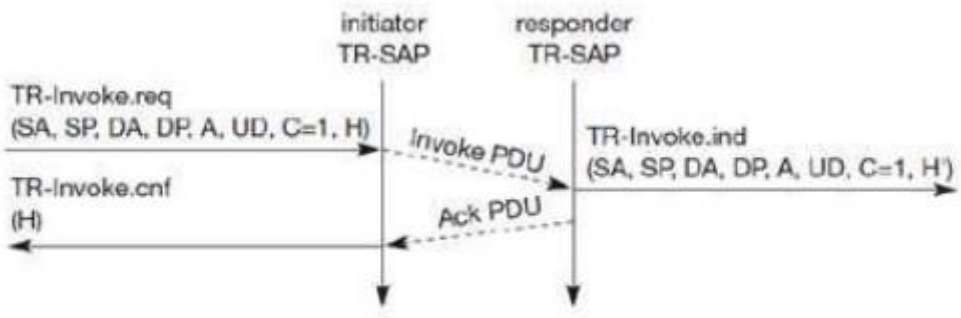


Fig 4.7 Basic Transaction , WTP Class 1, no user Acknowledgement

WTP class 2 finally, class 2 transaction service provides the classic reliable request/response transaction known from many client/server scenarios. Depending on user requirements, many different scenarios are possible for initiator/responder interaction.

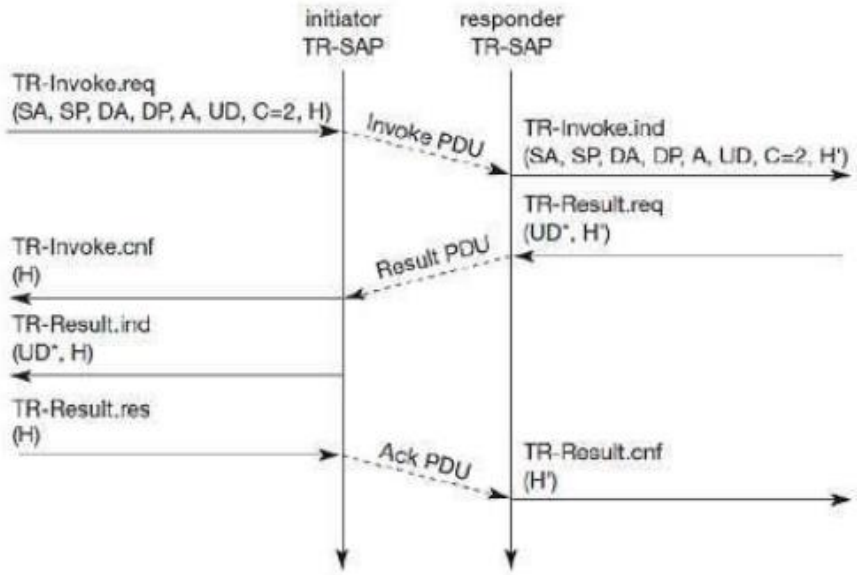


Fig 4.8 Basic Transaction , WTP Class 2, no user Acknowledgement

If the calculation of the result takes some time, the responder can put the initiator on ―hold on‖ to prevent a retransmission of the invoke PDU as the initiator might assume packet loss if no result is sent back within a certain timeframe.

6. WIRELESS SESSION PROTOCOL

Session Layer contains Wireless Session Protocol (WSP). It provides fast connection suspension and reconnection.

The **wireless session protocol (WSP)** has been designed to operate on top of the datagram service WDP or the transaction service WTP (WAP Forum, 2000e). For both types, security can be inserted using the WTLS security layer if required. WSP provides a shared state between a client and a server to optimize content transfer. HTTP, a protocol WSP tries to replace within the wireless domain, is stateless, which already causes many problems in fixed networks.

General features WSP

- **Session management:** WSP introduces sessions that can be **established** from a client to a server and may be long lived. Sessions can also be **released** in an orderly manner. The capabilities of **suspending** and **resuming** a session are important to mobile applications. Assume a mobile device is being switched off – it would be useful for a user to be able to

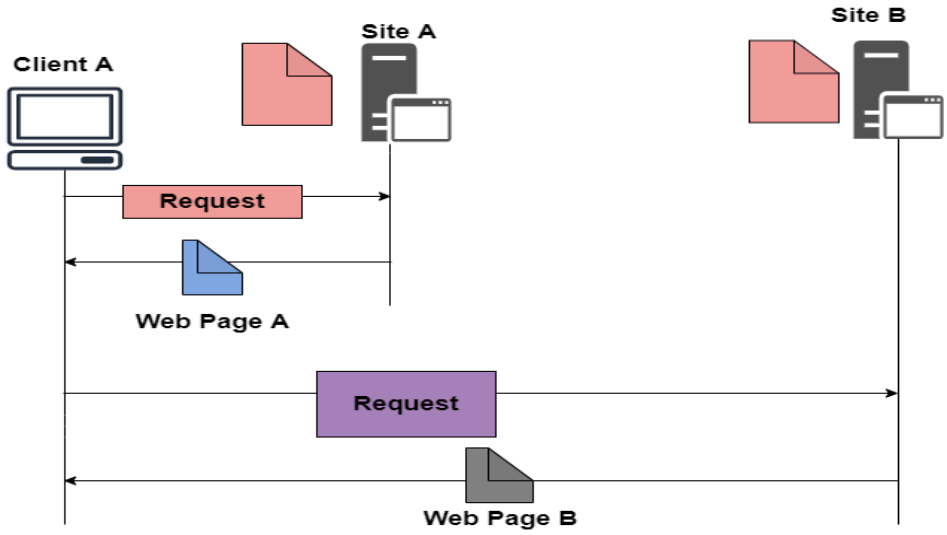
continue operation at exactly the point where the device was switched off. Session lifetime is independent of transport connection lifetime or continuous operation of a bearer network.

- **Capability negotiation:** Clients and servers can agree upon a common level of protocol functionality during session establishment. Example parameters to negotiate are maximum client SDU size, maximum outstanding requests, protocol options, and server SDU size.
- **Content encoding:** WSP also defines the efficient binary encoding for the content it transfers. WSP offers content typing and composite objects, as explained for web browsing. While WSP is a general-purpose session protocol, WAP has specified the **wireless session protocol/browsing (WSP/B)** which comprises protocols and services most suited for browsing-type applications.
- **Exchange of session headers:** Client and server can exchange request/reply headers that remain constant over the lifetime of the session. These headers may include content types, character sets, languages, device capabilities, and other static parameters. WSP/B will not interpret header information but passes all headers directly to service users.
- **Push and pull data transfer:** Pulling data from a server is the traditional mechanism of the web. This is also supported by WSP/B using the request/response mechanism from HTTP/1.1. Additionally, WSP/B supports three push mechanisms for data transfer: a confirmed data push within an existing session context, a non-confirmed data push within an existing session context, and a non-confirmed data push without an existing session context.
- **Asynchronous requests:** Optionally, WSP/B supports a client that can send multiple requests to a server simultaneously. This improves efficiency for the requests and replies can now be coalesced into fewer messages. Latency is also improved, as each result can be sent to the client as soon as it is available.

7. ARCHITECTURE OF WWW

The **World Wide Web** or Web is basically a collection of information that is linked together from points all over the world. It is also abbreviated as **WWW.** The **WWW** is mainly a distributed **client/server** service where a client using the browser can access the service using a server. The Service that is provided is distributed over many different locations commonly known as **sites/websites.**

- Each website holds one or more documents that are generally referred to as **web pages.**
- Where each web page contains a link to other pages on the same site or at other sites.
- These pages can be retrieved and viewed by using browsers.



In the above case, the client sends some information that belongs to **site A**. It generally sends a request through its browser (It is a program that is used to fetch the documents on the web).

and also the request generally contains other information like the address of the site, web page(URL).

The server at **site A** finds the document then sends it to the client. after that when the user or say the client finds the reference to another document that includes the web page at **site B**.

The reference generally contains the URL of site B. And the client is interested to take a look at this document too. Then after the client sends the request to the new site and then the new page is retrieved.

8. NETWORK SECURITY

Network security is the security provided to a network from unauthorized access and risks. It is the duty of network administrators to adopt preventive measures to protect their networks from potential security threats.

Computer networks that are involved in regular transactions and communication within the government, individuals, or business require security. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password.

Types of Network Security Devices

Active Devices

These security devices block the surplus traffic. Firewalls, antivirus scanning devices, and content filtering devices are the examples of such devices.

Passive Devices

These devices identify and report on unwanted traffic, for example, intrusion detection appliances.

Preventative Devices

These devices scan the networks and identify potential security problems. For example, penetration testing devices and vulnerability assessment appliances.

Unified Threat Management (UTM)

These devices serve as all-in-one security devices. Examples include firewalls, content filtering, web caching, etc.

Firewalls

- A firewall is a network security system that manages and regulates the network traffic based on some protocols. A firewall establishes a barrier between a trusted internal network and the internet.
- Firewalls exist both as software that run on a hardware and as hardware appliances. Firewalls that are hardware-based also provide other functions like acting as a DHCP server for that network..
- Firewalls are commonly used in private networks or *intranets* to prevent unauthorized access from the internet. Every message entering or leaving the intranet goes through the firewall to be examined for security measures.

Hardware and Software Firewalls

Hardware firewalls are standalone products. These are also found in broadband routers. Most hardware firewalls provide a minimum of four network ports to connect other computers. For larger networks − e.g., for business purpose − business networking firewall solutions are available. Software firewalls are installed on your computers. A software firewall protects your computer from internet threats.

Antivirus

An antivirus is a tool that is used to detect and remove malicious software. It was originally designed to detect and remove viruses from computers.

Modern antivirus software provide protection not only from virus, but also from worms, Trojan-horses, adwares, spywares, keyloggers, etc. Some products also provide protection from malicious URLs, spam, phishing attacks, botnets, DDoS attacks, etc.

9. EMAIL SECURITY

Email (short for electronic mail) is a digital method by using it we exchange messages between people over the internet or other computer networks. With the help of this, we can send and receive text-based messages, often an attachment such as documents, images, or videos, from one person or organization to another.

Steps to Secure Email:

We can take the following actions to protect our email.

- Choose a secure password that is at least 12 characters long, and contains uppercase and lowercase letters, digits, and special characters.
- Activate the two-factor authentication, which adds an additional layer of security to your email account by requiring a code in addition to your password.
- Use encryption, it encrypts your email messages so that only the intended receiver can decipher them. Email encryption can be done by using the programs like PGP or S/MIME.
- Keep your software up to date. Ensure that the most recent security updates are installed on your operating system and email client.
- **Beware of phishing scams:** Hackers try to steal your personal information by pretending as someone else in phishing scams. Be careful of emails that request private information or have suspicious links because these are the resources of the phishing attack.
- **Choose a trustworthy email service provider:** Search for a service provider that protects your data using encryption and other security measures.
- **Use a VPN:** Using a VPN can help protect our email by encrypting our internet connection and disguising our IP address, making it more difficult for hackers to intercept our emails.
- **Upgrade Your Application Regularly:** People now frequently access their email accounts through apps, although these tools are not perfect and can be taken advantage of by hackers. A cybercriminal might use a vulnerability, for example, to hack accounts and steal data or send spam mail. Because of this, it's important to update your programs frequently.

10. WEB SECURITY

Web Security is very important nowadays. Websites are always prone to security threats/risks. Web Security deals with the security of data over the internet/network or web or while it is being transferred to the internet. For e.g. when you are transferring data between client and server and you have to protect that data that security of data is your web security.

Hacking a Website may result in the theft of Important Customer Data, it may be the credit card information or the login details of a customer or it can be the destruction of one's business and propagation of illegal content to the users while somebody hacks your website they can either steal the important information of the customers or they can even propagate the illegal content to your users through your website so, therefore, security considerations are needed in the context of web security.

Security Threats:
A Threat is nothing but a possible event that can damage and harm an information system. Security Threat is defined as a risk that which, can potentially harm Computer systems & organizations. Whenever an Individual or an Organization creates a website, they are vulnerable to security attacks.

Security attacks are mainly aimed at stealing altering or destroying a piece of personal and confidential information, stealing the hard drive space, and illegally accessing passwords. So whenever the website you created is vulnerable to security attacks then the attacks are going to steal your data alter your data destroy your personal information see your confidential information and also it accessing your password.

Top Web Security Threats :
Web security threats are constantly emerging and evolving, but many threats consistently appear at the top of the list of web security threats. These include:

- Cross-site scripting (XSS)
- SQL Injection
- Phishing
- Ransomware
- Code Injection
- Viruses and worms
- Spyware
- Denial of Service

~~~~~~~~~ All the Best ~~~~~~~