**Advanced Topics on Networks**

**Assignment 1**

**Q1: Define the following terms:**

1. Forwarding

move packets from router’s input to appropriate router output.

1. Routing

determine route taken by packets from source to dest.

1. Virtual Circuits

source-to-dest path behaves much like telephone circuit

1. Network Layer Functions

transport segment from sending to receiving host, on sending side encapsulates segments into datagrams, on rcving side, delivers segments to transport layer, network layer protocols in every host, router, router examines header fields in all IP datagrams passing through it.

1. Datagram Networks

no call setup at network layer, routers: no state about end-to-end connections, packets forwarded using destination host address.

1. IP address

32-bit identifier for host, router interface

1. Interface

connection between host/router and physical link

1. NAT Motivation

local network uses just one IP address as far as outside world is concerned.

1. IP V6 Initial Motivation

32-bit address space soon to be completely allocated.

1. IP V6 Additional Motivations

header format helps speed processing/forwarding , header changes to facilitate QoS.

1. Area border routers

“summarize” distances to nets in own area, advertise to other Area Border routers.

1. Backbone routers

run OSPF routing limited to backbone.

1. Boundary routers

connect to other AS’s

1. Flooding

when node receives brdcst pckt, sends copy to all neighbors.

1. Broadcast Routing

deliver packets from source to all other nodes , source duplication is inefficient.

1. Source-based tree

one tree per source, shortest path trees,

1. Group-shared tree

reverse path forwarding

1. Priority (IPv6 header field)

identify priority among datagrams in flow

1. Flow Label (IPv6 header field)

identify datagrams in same “flow.”

1. Next header (IPv6 header field)

identify upper layer protocol for data

1. Poison reverse

used to prevent ping-pong loops (infinite distance = 16 hops).

**Q2: State and define the IP header fields.**

is header information at the beginning of an Internet Protocol (IP) packet

The header fields are discussed below: Version (always set to the value 4 in the current version of IP).

**Q3: Using the data below to describe how the fragmentation process will be achieved.**

**Datagram Size: 3820 MTU Size: 820**

|  |  |  |  |
| --- | --- | --- | --- |
| Fvag fleg | offset | ID | large |
| 0 | 0 | x | 3820 |

One large datagram will be fragmented to several datagrams.

Datagram without header 3820-20= 33800

Header = 20b4tes

Data field size= MTU – header= 820-20- 800 bytes

a)offset= Data + header = 800 + 20 = 820

|  |  |  |  |
| --- | --- | --- | --- |
| large | ID | Flag | Offset |
| 820 | X | 1 | 0 |

b)Offset = 800/8 = 100

|  |  |  |  |
| --- | --- | --- | --- |
| Large | ID | Flag | Offset |
| 820 | X | 1 | 100 |

c) Offset= (800+800)/8 = 1600/8=200

|  |  |  |  |
| --- | --- | --- | --- |
| large | ID | Flag | Offset |
| 820 | X | 1 | 200 |

d)Offset= (800+800+800 /8 = 2400/8 = 300

|  |  |  |  |
| --- | --- | --- | --- |
| large | ID | Flag | Offset |
| 820 | X | 1 | 300 |

e)Offset= (800+800+800+800) /8 = 400 Flag = 0 be caves it is The last fragment

|  |  |  |  |
| --- | --- | --- | --- |
| large | ID | Flag | Offset |
| 620 | X | 0 | 400 |

**Q4: State the NAT advantages**

* devices inside local net not explicitly addressable, visible by outside world (a security plus).
* can change ISP without changing addresses of devices in local network
* can change addresses of devices in local network without notifying outside world
* range of addresses not needed from ISP: just one IP address for all devices

**Q5: Compare between IPv4 and IPv6**

|  |  |
| --- | --- |
| IPv4 | IPv6 |
| IPv4 addresses are 32 bit length. | [**IPv6 addresses**](http://www.omnisecu.com/tcpip/ipv6/introduction-to-ipv6-addressing.php) **are 128 bit length.** |
| [IPv4 addresses](http://www.omnisecu.com/tcpip/internet-layer-ip-addresses.php) are [binary numbers](http://www.omnisecu.com/tcpip/binary-decimal-hexadecimal-numbers-and-conversions.php) represented in decimals. | [**IPv6 addresses**](http://www.omnisecu.com/tcpip/ipv6/introduction-to-ipv6-addressing.php)**are**[**binary numbers**](http://www.omnisecu.com/tcpip/binary-decimal-hexadecimal-numbers-and-conversions.php)**represented in**[**hexadecimals**](http://www.omnisecu.com/tcpip/binary-decimal-hexadecimal-numbers-and-conversions.php)**.** |
| [IPSec](http://www.omnisecu.com/security/ipsec/index.php) support is only optional. | **Inbuilt [IPSec](http://www.omnisecu.com/security/ipsec/index.php) support.** |
| [Fragmentation](http://www.omnisecu.com/tcpip/internet-layer.php) is done by sender and forwarding routers. | [**Fragmentation**](http://www.omnisecu.com/tcpip/internet-layer.php)**is done only by sender.** |
| No packet flow identification. | **Packet flow identification is available within the**[**IPv6 header**](http://www.omnisecu.com/tcpip/ipv6/ipv6-datagram-header-format.php)**using the**[**Flow Label**](http://www.omnisecu.com/tcpip/ipv6/ipv6-datagram-header-format.php)**field.** |
| [Checksum field](http://www.omnisecu.com/tcpip/internet-layer.php) is available in [IPv4 header](http://www.omnisecu.com/tcpip/internet-layer.php) | **No checksum field in**[**IPv6 header**](http://www.omnisecu.com/tcpip/ipv6/ipv6-datagram-header-format.php)**.** |
| [Options fields](http://www.omnisecu.com/tcpip/internet-layer.php) are available in [IPv4 header](http://www.omnisecu.com/tcpip/internet-layer.php). | **No option fields, but**[**IPv6 Extension headers**](http://www.omnisecu.com/tcpip/ipv6/ipv6-datagram-header-format.php)**are available.** |
| [Address Resolution Protocol (ARP)](http://www.omnisecu.com/tcpip/address-resolution-protocol-arp.php) is available to map [IPv4 addresses](http://www.omnisecu.com/tcpip/internet-layer-ip-addresses.php) to [MAC addresses](http://www.omnisecu.com/tcpip/media-access-control-mac-addresses.php). | [**Address Resolution Protocol (ARP)**](http://www.omnisecu.com/tcpip/address-resolution-protocol-arp.php)**is replaced with a function of**[**Neighbor Discovery Protocol (NDP)**](http://www.omnisecu.com/tcpip/ipv6/ndp-neighbour-discovery-protocol-functions-of-ndp.php)**.** |
| Internet Group Management Protocol (IGMP) is used to manage multicast group membership. | **IGMP is replaced with Multicast Listener Discovery (MLD) messages.** |
| [Broadcast messages](http://www.omnisecu.com/cisco-certified-network-associate-ccna/unicast-multicast-broadcast.php) are available. | [**Broadcast messages**](http://www.omnisecu.com/cisco-certified-network-associate-ccna/unicast-multicast-broadcast.php)**are not available.** |
| Manual configuration (Static) using DHCP (Dynamic configuration). | **Auto-configuration of addresses is available.** |

**Q6: State the Tunneling process.**

is the quantum mechanical phenomenon where a wavefunction can propagate through a potential barrier. ... The wave function and its first derivative are continuous. In steady state the probability flux in the forward direction is spatially uniform. No particle or wave is lost.

**Q7: Using example to describe how the advertisements is useful in RIP routing process.**

All Routers send an advertisement that contains its forwarding table to all its neighbors routers such as Router A send response message with its forwarding table to Router D so based on this advertisements Router D choose the route to subnets with the least distance Router D finds the route with least distance to sunet Z is 5 instead of 7 through the router.

**Q8: State the RIP Link Failure and Recovery.**

If no advertisement heard after 180 sec --> neighbor/link declared dead**.**

routes via neighbor invalidated >> new advertisements sent to neighbors >> neighbors in turn send out new advertisements (if tables changed) >> poison reverse used to prevent ping-pong loops (16 hops).

**Q9: State the OSPF “advanced” features which are not found in RIP.**

* Security
* multiple same-cost paths allowed (only one path in RIP)
* integrated uni- and multicast support
* hierarchical OSPF in large domains
* For each link, multiple cost metrics for different TOS

**Q10: State BGP functions.**

1. Obtain subnet reachability information from neighboring ASs.
2. Propagate reachability information to all AS-internal routers.
3. Determine “good” routes to subnets based on reachability information and policy.

**Q11: State the difference between eBGP and iBGP.**

**eBGP** :Obtain subnet reachability information from neighboring ASs.

**iBGP:** Propagate reachability information to all AS-internal routers

**Q12: State and define the two important attributes in BGP.**

1-AS-PATH: contains ASs through which prefix advertisement has passed

**2-** NEXT-HOP: indicates specific internal-AS router to next-hop AS.

**Q13: State the routing paths elimination rules**

1- local preference value attribute: policy decision

2- shortest AS-PATH

3- closest NEXT-HOP router: hot potato routing

4- additional criteria

**Q12: State and define the BGP messages.**

BGP messages exchanged using TCP

* OPEN: opens TCP connection to peer and authenticates sender
* UPDATE: advertises new path (or withdraws old)
* KEEPALIVE keeps connection alive in absence of UPDATES; also ACKs OPEN request
* NOTIFICATION: reports errors in previous msg; also used to close connection

**Q13: Describe with example the BGP routing policy.**

Applying Routing Policies
to BGP

**Q14: State the difference Intra- and Inter-AS routing.**

Inter-AS: admin wants control over how its traffic routed, who routes through its net.

Intra-AS: single admin, so no policy decisions needed

**Q15: State the steps which are used for nodes to join the Center-based trees.**

1. edge router sends unicast join-msg addressed to center router
2. join-msg “processed” by intermediate routers and forwarded towards center
3. join-msg either hits existing tree branch for this center, or arrives at center
4. path taken by join-msg becomes new branch of tree for this router