Advanced Topics on Networks

Assignment 1

Q1: Define the following terms:

1. Forwarding : move packets from router's input to appropriate router output.
2. Routing: determine route taken by packets from source to dest.
3. Virtual Circuits : source-to-dest path behaves much like telephone circuit
4. 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.
5. Datagram Networks: no call setup at network layer, routers: no state about end-to-end connections, packets forwarded using destination host address.
6. IP address : 32-bit identifier for host, router interface,
7. Interface : connection between host/router and physical link
8. NAT Motivation : local network uses just one IP address as far as outside world is concerned.
9. IP V6 Initial Motivation : 32-bit address space soon to be completely allocated.
10. IP V6 Additional Motivations : header format helps speed processing/forwarding , header changes to facilitate QoS.
11. Area border routers : "summarize" distances to nets in own area, advertise to other Area Border routers.
12. Backbone routers : run OSPF routing limited to backbone.
13. Boundary routers : connect to other AS's
14. Flooding : when node receives brdcst pckt, sends copy to all neighbors.
15. Broadcast Routing : deliver packets from source to all other nodes , source duplication is inefficient.
16. Source-based tree : one tree per source, shortest path trees,
17. Group-shared tree : reverse path forwarding
18. Priority (IPv6 header field) : identify priority among datagrams in flow
19. Flow Label (IPv6 header field) : identify datagrams in same "flow."
20. Next header (IPv6 header field) : identify upper layer protocol for data
21. Poison reverse : used to prevent ping-pong loops (infinite distance = 16 hops).

Q2: State and define the IP header fields.

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

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

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 are 128 bit length.
IPv4 addresses are binary numbers represented in decimals.	IPv6 addresses are binary numbers represented in hexadecimals.
IPSec support is only optional.	Inbuilt IPSec support.
Fragmentation is done by sender and forwarding routers.	Fragmentation is done only by sender.
No packet flow identification.	Packet flow identification is available within the IPv6 header using the Flow Label field.
Checksum field is available in IPv4 header	No checksum field in IPv6 header.
Options fields are available in IPv4 header.	No option fields, but IPv6 Extension headers are available.
Address Resolution Protocol (ARP) is available to map IPv4 addresses to MAC addresses.	Address Resolution Protocol (ARP) is replaced with a function of Neighbor Discovery Protocol (NDP).
Internet Group Management Protocol (IGMP) is used to manage multicast group membership.	IGMP is replaced with Multicast Listener Discovery (MLD) messages.
Broadcast messages are available.	Broadcast messages are not available.
Manual configuration (Static) using DHCP (Dynamic configuration).	Auto-configuration of addresses is available.

Q6: State the Tunneling process.

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

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.

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