# Solutions to Review Questions #1

Covers: Udacity Lessons 1-5.2 and associated readings

## Architecture and Principles

1. **How does the "narrow waist" allow a large variety of different protocols to be used on the Internet?**

By standardizing the way traffic is routed between networks (i.e., everyone must use IP), it opens the way for different protocols to be used at both higher and lower layers. Because IP is responsible for moving traffic between networks (at layer 3), each network may use any technology they choose (at layers 1 & 2) to move traffic within their network, and data can still traverse the Internet because IP glues the different networks together. At the same time, higher layers (e.g., transport & application layers) operate strictly end-to-end. Since the standard protocol for the Internet (IP) works in the core of the network, any end-to-end services may be built on top of it.

2. **Discuss how the design principles of the Internet are manifest in the ARP protocol. Also discuss how the absence of some points from the design principles (e.g., security and mobility) has influenced ARP.**

The fundamental design goal is to connect the disparate individual (layer 2) networks by inter-networking them with IP (at layer 3). ARP plays a key role in this by translating between the different addressing schemes of IP (at layer 3) and Ethernet (at layer 2). End-to-end communication is addressed by IP addresses because the sender and receiver may not be in the same local (layer 2) network. Internet communication are dependent on the local (layer 2) network being able to deliver packets within that network, but layer 2 networks use different addressing schemes – MAC addresses, in the case of Ethernet. Thus some mechanism is needed to find the MAC address of a machine, thus allowing the local network to direct traffic, based on knowing the IP (layer 3) address of the machine. ARP fill this role for Ethernet networks.

The Internet architecture must accommodate a variety of networks. This relates to the above, but specifically illustrates why different addresses may be used at layers 2 and 3 – not all local networks are Ethernets or use MAC addresses. The narrow waist dictates that all Internet networks must use IP addressing at layer 3, but different types of networks may use different layer 2 addressing.

Fate sharing, or Internet communication must continue despite loss of networks or gateways. ARP does not use any centralized authority for storing IP→MAC mappings, but rather is a distributed protocol that allows each machine to be responsible for answering queries about the IP→MAC mappings for its own IP addresses. This means that the failure of any host only makes that hosts' IP→MAC mapping inaccessible, and in such a situation, communication with that host would not be possible anyway. Furthermore, any failure in the network core does not

disrupt a host from discovering the IP→MAC mapping of another host unless that network failure would necessarily disrupt communication between those two hosts anyway.

The Internet architecture must permit distributed management of its resources. This is also true because ARP does not use any centralized authority for storing IP→MAC mappings.

The Internet architecture must permit host attachment with a low level of effort. ARP allows for IP→MAC mapping discovery dynamically, on an as-needed basis. Thus there is no need for a machine's IP→MAC mappings to be proactively reported to other hosts on the network. This eliminates any administrative burden in disseminating IP→MAC mappings that might make it harder to add a machine to a network. (Together with switch self-learning and protocols such as DHCP that assist joining a network at layer 3, the makes adding a host to a network zero-configuration in most cases, and minimal-configuration in others.)

Other points may also be possible. This is just a sampling of some of the key points.

3. **What are the advantages of using circuit-switched networks instead of packet-switched networks (like the Internet) for streaming video?**

The biggest advantage is guaranteed bandwidth, which assures that sufficient throughput will be available for the video, and further guarantees that throughput won't be affected by other users'/applications' traffic on the network. Although this cannot eliminate all possible source of packet loss, the ability to reserve sufficient resources for the video traffic can eliminate one of the major sources of packet loss. Finally, certain streaming video applications (most especially interactive ones, such as VoIP / video conference) may benefit from the upper bounds on latency that circuit switched networks can provide.

4. **In what way are caching HTTP proxies a violation of the end-to-end argument? Also, what are the consequences of this?**

HTTP proxies divert web requests from their stated destination (web server) to the proxy, which is likely closer to the requester (client/browser) and can respond with less latency, providing the same content. While this is often desirable for its performance gains, it is technically a violation of the end-to-end argument because the remote host you end up talking to is not the one that you stated you wanted to talk to (even though the content it provides did originally come from that source).

A consequence of this is that, while encryption can be used to secure the traffic between the proxy and the client, end-to-end encryption between the client and the original web server (the one that the client actually stated it wanted to talk to) is not possible while the proxy is acting as an intermediary. While this still protects against attacks from other outside parties, identification is an important part of secure communication, and the original web server cannot identify itself to the client while the proxy acts as an intermediary. The proxy could identify itself, but additional mechanisms would be needed to verify that the proxy is indeed authorized to act on behalf of the original web server. (Even then, the client must trust that the proxy is well constructed and does not leave security holes open when it communications with the

original web server that may allow attackers to inject bad content into the proxy in place of the web server's true content.)

5. **Why is it important for encryption to be end-to-end? In other words, what are the consequences if we perform encryption, but not in an end-to-end manner?**
    a. **(Bonus question: Gmail uses HTTPS to secure communication between your browser and the Gmail servers. Is this encryption "end-to-end"?)**

Encryption could be performed at every step without being provided end-to-end, for example, each link that traffic traverses could independently encrypt the data during transmission. However, the means that intermediate routers will see the traffic, as it is sent encrypted over one link to the router, decrypted, then re-encrypted to go over the next link. This requires trust in those routers, but such trust may not be advisable due to the distributed management of the Internet – these routers are managed by many different organizations. Furthermore, neither the sender nor receiver can guarantee which routers (and therefore which organizations) their traffic will or will not traverse.

This may be further exacerbated by attackers who could make themselves a man-in-the-middle by posing as a legitimate router and enticing traffic to flow through them – since they would get to decrypt and re-encrypt everything, they will get to see the cleartext (i.e., unencrypted message) of all the supposedly-encrypted traffic. Another approach for an attacker would be to hack a legitimate router and bring it under the attacker's control.

Finally, identification is a critical component of any reliable encryption system. If the other end does not identify themselves, you may know that you have secure communication with the other end, but do not know if you are talking to who you want to talk to, or a hacker posing as that host. However, piecewise encryption makes it difficult to verify the identity of the other end, or indeed any of the intermediate steps (making the previous paragraph possible) other than the one very first hop router (which could identify itself to the sender). Thus a hacker could not only be a man-in-the-middle by posing as an intermediate router, but also by posting as the other end host, i.e., the intended receiver.

Whether Gmail encryption is "end-to-end" is subjective, since it depends on who you consider to be "the end". However, we might argue that it is not because we could claim that the "ends" are the sender and receiver of the email. Even if both of them use encrypted connections to talk to Gmail's servers, the email is visible to Google itself. In order to provide true end-to-end encryption for email, an email encryption system would be required that encrypts the email itself with keys known only* to the sender & receiver, rather than encrypting the individual connection between a user's browser and Gmail's servers.

( * slight oversimplification since we would likely use asymmetric key encryption for email encryption, but we don't need to worry about that detail for this discussion if you're not very familiar with asymmetric key encryption)

6. **The forwarding tables for all switches in this network are initially empty. Host 192.168.1.1 sends and ARP request to discover the MAC address of the host with IP 192.168.1.2. What entries will be in the forwarding table of each switch after host 192.168.1.1 receives the ARP reply?**

(figure omitted – see the questions document for the network diagram)

| **Switch** | **Dest MAC** | **Out Port** |
|---|---|---|
| sw1 | AA:AA:AA:AA:AA:AA<br>BB:BB:BB:BB:BB:BB | 3<br>2 |
| sw2 | AA:AA:AA:AA:AA:AA | 1 |
| sw3 | AA:AA:AA:AA:AA:AA<br>BB:BB:BB:BB:BB:BB | 1<br>2 |
| sw4 | AA:AA:AA:AA:AA:AA<br>BB:BB:BB:BB:BB:BB | 2<br>1 |

7. **When a host on the private network side of a NAT with IP 192.168.1.100 opens a TCP connection to a web server at 123.45.67.89, what entry will be added to the following NAT table, and what will be the source and destination IP and port on the packet that the NAT router forwards on the WAN (public) side? (Recall that the default port for HTTP is port 80.)**

| Public IP | Public Port | Private IP | Private Port |
|---|---|---|---|
| 98.76.54.32 | 35564 | 192.168.1.100 | 22 |
| 98.76.54.32 | 5416 | 192.168.1.101 | 80 |
| 98.76.54.32 | 15885 | 192.168.1.105 | 6843 |
| 98.76.54.32 | 4321 * | 192.168.1.100 | 12345 ** |

* generated automatically by NAT router from available/unused port numbers (your number may vary, as long as you explain where it came from)

** generated automatically by the client host when it begins to open a new connection to the server, chosen from available/unused “ephemeral” ports (your number may vary, as long as you explain where it came from)

| Dst IP | Dst Port | Src IP | Src Port |
|---|---|---|---|
| 123.45.67.89 | 80 | 98.76.54.32 | 4321 * |

* your number may vary here, but it should be the same one marked with single-* above

8. **How does the Spanning Tree Protocol (STP) improve the reliability of Ethernets?**

Failures can happen in a physical network. Cables go bad, switches have hardware failures, people dig where they shouldn't and cut underground cables, etc. In order to prevent such individual failures from causing a failure in the overall network (e.g., these may lead to network partitioning), it is desirable to have redundant links in the network. However, redundant links cause problems in broadcast networks, namely that they cause flooded messages not only to loop forever but also to replicate themselves and magnify the bad traffic in an effect known as a "broadcast storm". Even in switched Ethernet, some packets still get flooded, for example when a switch has not yet learned about a destination MAC, or if there is a deliberate broadcast message, such as an ARP request.

What STP allows is redundant links in the physical layer without any loops in the logical network by calculating a loop-free, fully connected subset of network links (i.e., a spanning tree) that will be used and the other, redundant links can be disabled at the link layer. In the event of a failure, disabled links can easily be re-enabled as part of a new spanning tree, thus keeping the network connected and functional, but without needing human intervention at the physical layer (e.g., plugging/unplugging cables).

9. **Explain why 2T*C represents the number of outstanding bits (or bits "in flight") for a TCP flow. (Note: another way to write this would be RTT*C )**

TCP implements congestion control by limiting the number of outstanding bits; this limit is called the congestion window (which is actually expressed in a number of bytes, not bits, but we'll assume appropriate unit conversion happen here). When a packet is sent, it is considered outstanding until the sender receives an ACK for that packet. So if it can send W, the window size, bits every time those bits are acknowledged, that makes the rate it sends W/RTT (note how the units are bps). Congestion control sets the window size appropriately so the sending rate meets the bottleneck as well as possible without exceeding it. Therefore the bottleneck rate, C = W/RTT, which we can rewrite as W = RTT*C. Since the window size W is the amount of data that can be outstanding, we know that the outstanding data is RTT*C (or 2T*C).

Note that this only applies to TCP! Since UDP does not have congestion control, it does not receive ACKs and will send as fast as the application code tells it to. So the number of outstanding packets for a UDP flow is not necessarily limited by 2T*C. However, TCP is so much more common than UDP on the Internet, that we can make decisions based on TCP assumptions (such as buffer sizing) that basically still hold true in the real world where both TCP and UDP are used.

10. **Suppose a particular router normally supports 1000 flows at a time. The average round-trip time (RTT) of each flow is 63ms, and the bottleneck link is 5 Mbps. According to the new thinking on buffer sizes (i.e., Appenzeller 2004), what size should the buffer on this router be?**

The buffer size should be 2T*C / sqrt(n), or RTT*C / sqrt(n).

5Mbps * 63ms / sqrt(1000)

5*1000*1000 bps * 0.063 sec / sqrt(1000)

315,000 bits / sqrt(1000)

9961.17 → 9962 bits

9962 / 8 = **1246 bytes = 1.217 kB**

**Reading - DARPA Internet Protocols**

11. **Discuss the advantages of the fate-sharing survivability model present in Internet Protocols today, and how this model differs from a distributed state/replicated survivability model.**

Fate-sharing protects against a number of intermediate failures, because intermediate packet switching nodes between the end-points of communication do not contain state information. For example, consider two hosts communicating across a large network with many intermediate nodes. Any number of these intermediate nodes may fail, and as long as the failures do not result in a partitioning of the network, the two hosts can continue to communicate within the context of the same state.

In contrast, a distributed/replicated state model where state information regarding a connection between two endpoints is contained within some subset of all intermediate nodes in the network can only survive a certain number of failures, one less than the minimum number of intermediate nodes required to hold the state.

Additionally, a fate-sharing model is far easier to implement than a replicated model. Transport layer synchronization information need only be engineered in the hosts, not every intermediate network node. Additionally, network based replication algorithms and subroutines are not required.

12. **Explain how the Internet architecture achieves the flexibility required to support a wide variety of networks? What functions is the network assumed to provide, and more importantly, what functions of the network are NOT assumed?**

The architecture of the Internet achieves flexibility by making the minimum number of assumptions possible about the functions the network provides to hosts on the network. This philosophy creates a ubiquitous Internet layer (the narrow waist) that permits varied networks with different properties and purposes to all connect to a common Internet.

It is assumed that the network can transport a packet of reasonable size, with reasonable reliability. Further, it is also assumed that the network provides a suitable method for addressing hosts on the network.

It is NOT assumed that the network provides services like guaranteed delivery, sequenced delivery, network level broadcast/multicast, prioritization of traffic, or maintain information like internal network state (failures, speeds, delays, etc.). If these assumptions about the network are made, then networks wishing to connect to the internet that do not accommodate these assumptions must be reengineered

13. **How has the ARPANET design goal of distributed resource management across the network not been met in today's Internet?**

Internet gateways are not all managed by a single management entity. Gateway administered by different authorities cannot fully "trust" each other, and use a variety of mechanisms to exchange routing information both externally and internally. In some cases, an authority managing a gateway may not be the same as the authority managing the network attached to that gateway.

Additionally, distributed management tools are insufficient to manage even basic services, like routing. In many cases routing decisions are still manually controlled at various levels by different administrative authorities. These manual processes are very prone to human error, and require significant resources to maintain.

14. **Describe two of the design advantages of datagrams as the basic architectural feature of the Internet.**

Possible answers include:

No need for connection state: This supports the design principle of flexibility for varieties of networks, as datagrams do not require connection state within the network's intermediate nodes to be routed. Datagrams provide desirable survivability (fate-sharing) properties.

Basic building blocks: The datagram is intentionally designed to be an elemental building block upon which many different types of service can be built. This supports the design principle of supporting a wide variety of services. Endpoints on the network can take advantage of the datagram design to create a service specific to that host's transport or application level needs.

Minimum network assumption: As discussed in 12, the datagram is a manifestation of the minimum level of assumptions made about services provided by the network. It permits a wide variety of networks to connect to the Internet at large.

Incorrect Answer: Datagrams were selected as an architectural feature in order to permit higher level services (like TCP or HTTP) to connect on the network.

These higher level services do not require datagrams, they are built on top of them.

**Reading - End to End Arguments**

15. **Consider a networked application that is latency sensitive and requires guaranteed delivery and of data packets between network hosts. Assume that errors in transmission are very rare. Would a network that violates the end-to-end principle by implementing packet acknowledgements and checksums within the low-level network architecture be a suitable choice for this application?**

No. Any network based internal low-level packet acknowledgements and checksums would reduce available bandwidth (from point to point acknowledgement overhead) and increase latency (point to point checksums), likely to the point where the application would not be able to tolerate these performance losses. This is exacerbated by the fact that the no matter how reliable the network is, an end to end check of data is still required. Therefore there is no offsetting reduction in complexity by the host to accommodate this performance loss in the network.

16. **Describe how the end-to-end argument supports clear definitions between network layers? ( i.e. why is reliable, in-order delivery packets a feature of a transport layer protocol and not the internet layer? Why is IP a connectionless protocol?)**

Without clearly defined criteria for determining what functions belong in which layers, the modularity benefits of "layering" are not achieved. The end-to-end argument provides principles for the organization of these systems.

For example, the Internet layer achieves the goals of the ARPANET design principles of supporting a wide variety of services and networks by following the end to end argument. This narrow waist includes the minimum amount of end-to-end functionality, allowing the transport and application layers to include functions like guaranteed delivery, in-order delivery, efficient file transfers, etc.

**<u>IP Addressing & Forwarding</u>**

17. **Consider a subnet that has the following IP addresses. What is the smallest subnet (i.e., subnet with the longest prefix) that could include all these addresses? (Use CIDR, i.e. "slash", notation.)**

192.168.165.1
192.168.165.96
192.168.160.1
192.168.179.145

192.168.160.0/19

In the third place, 165, 160, and 179 all start with binary 101… but the fourth binary digit differs: 160 and 165 both start with 1010… but 179 starts with 1011… so we have all 8 digits of the first part, all 8 digits of the second part, and 3 digits of the third part. 8+8+3=19, so it's a /19 subnet.

18. **How many addresses are in the subnet 10.11.12.128/26 ? (Show your work.)**

There are 2^(32-26) addresses in a /26 subnet. 2^(32-26) = 2^6 = **64**

**19. Now consider a router with the following forwarding table:**

| Subnet | Next Router | Cost |
|---|---|---|
| 73.214.32.0/20 | 192.168.1.1 | 3 |
| 73.214.0.0/16 | 192.168.2.1 | 4 |
| 73.214.42.0/24 | 192.168.3.1 | 5 |
| 73.214.37.0/24 | 192.168.4.1 | 6 |

( Note: 42 = 32 + 8 + 2 and 37 = 32 + 4 + 1 )

a. **To which router will a datagram with destination IP address 73.214.106.198 be sent next?**

192.168.2.1 because 73.214.0.0/16 is the only match

b. **To which router will a datagram with destination IP address 73.214.42.64 be sent next?**

192.168.3.1 because 73.214.42.0/24 is a longer prefix than 73.214.0.0/16 or 73.214.32/20

c. **To which router will a datagram with destination IP address 73.214.39.216 be sent next?**

192.168.1.1 because 73.214.32.0/20 is a longer prefix than 73.214.0.0/16

**<u>Routing</u>**

**20. Consider this network and the Distance Vector algorithm:**

**(Figure Omitted)**

**What does router D update its distance vector to?**

| A | B | C | D | E | F |
|---|---|---|---|---|---|
| 1 | 3 | **4** | 0 | 3 | **6** |
| | | | | | |

**21. Suppose you are operating an enterprise network (such at Georgia Tech's network, or a medium-sized corporation's network) and you decide to use RIP for your intra-AS routing. List two advantages that using RIP gives you (in contrast to using OSPF or IS-IS).**

One advantages is that RIP requires little to no configuration (i.e., configuring the routers to use RIP), so it can work correctly right out of the box. Another advantage is that Distance Vector

routing (which RIP uses to calculate routes) dynamically responds to changes in the network, such as changes to the topology. (In contrast, a Link State protocol such as OSPF or IS-IS has to wait until the next "round" of recomputing routes before any changes are accounted for.)

**22. List two reasons for using Autonomous Systems (AS) in the Internet.**

ASes make Internet routing more scalable by introducing a level of hierarchy above individual networks. Thus intra-AS routing protocols don't have to scale to the size of the entire Internet, and BGP (the inter-AS protocol) doesn't either because it routes on the whole-AS granularity.

Another reason is that it gives organizations administrative control over their own networks (i.e., the networks within the AS that they own). This allows them no only to choose whichever intra-AS routing protocol they like, but also to set and enforcing routing policies for their AS.

**23. BGP provides three ways for network operators to enforce policies on their networks. List these ways.**

They can set the "local preference" (LOCAL_PREF) field on BGP messages in their networks.

They can choose whether or not to share advertisements with neighbor ASes (i.e., whether to send an eBGP message for a route they know about).

They can choose whether or not to accept advertisements from neighbor ASes (i.e., whether or not to send iBGP messages to the rest of their network for a route advertisement received from a neighbor AS).

**<u>Other Network Layer Protocols</u>**

**24. In an Internet where some routers are IPv6 routers (i.e., they support both IPv6 and IPv4) but most are IPv4 routers (that support only IPv4), how can two hosts communicate with each other using IPv6? (In other words, how can IPv6 be used if not all the routers are IPv6 routers?)**

IPv6 can tunnel through IPv4. That means that IPv6 forwarding finds the next IPv6 router to send the packet to, and IPv4 is used to send the packet from one IPv6 router to the next. This is done by encapsulating the IPv6 packet inside an IPv4 packet, where the IPv4 destination is the IPv4 address of the next IPv6 router, while the IPv6 destination is the actual final destination of the packet. (Of course the end host sender and receiver do need to support IPv6 for this to work at all.)

**25. Explain the ways in which DNS (the Domain Name System) achieves fault-tolerance, i.e., such that most or all domain names can be resolved to IP addresses even if some (but not all) DNS servers crash.**

1. Replication exists at all levels of the hierarchy, such as the 13 root servers, and the requirement to have at least 2 authoritative servers for every domain. This means that records remain accessible even if N-1 of the N replicas go down.
2. Partitioning provides fate sharing. If a domain's authoritative servers go down, the records for other domains can still be accessed. Also, if the TLD server of one TLD goes down, the other TLDs' records are still accessible.
3. Caching in the local server (and in some cases, on the end host) can keep cached records available even if the authoritative server is down.

**26. Consider a NAT router with the following entry in its translation table:**


a. **What does the NAT router do when it receives a packet on the WAN (Internet) interface with the destination address/port 138.76.29.7:5001?**

The NAT router rewrites the destination address/port on the packet to 10.0.0.1/3345 and transmits the packet on the LAN-side interface.

b. **What does the NAT router do when it receives a packet on the LAN (Local Area Network) interface with the source address/port 10.0.0.1:3345?**

The NAT router rewrites the source address/port on the packet to 138.76.29.7/5001 and transmits the packet on the WAN-side interface.

c. **How does this entry get added to the NAT router's translation table? (Assume the client is on the LAN side and the server is on the WAN side.)**

When the LAN side sends the first SYN packet to the server, beginning the process of establishing a TCP connection, the NAT router writes the entry in it's table. The private-side (or LAN-side) address/port are the sender's address/port on this packet. The public-side (or WAN-side) IP address is the public IP address for this NAT network, and the public-side port number is selected by the NAT router from among those not already in use.

Other methods exist, such as static entries that are created by the NAT router's administrator, or protocols such as STUN that tell the router what to use. However, automatically creating entries upon TCP connection is by far the most common way it's done.

**27. What is the difficulty with hosting a server (e.g. a web server) behind a NAT router (i.e. on the LAN side)?**

When the client sends a SYN packet, the packet comes from the private side of the client's NAT, so the address/port in the packet is the address/port to use in the translation table. However, if a server is behind a NAT, then the SYN packet would come from the public side. Since the public address had to be used to forward the packet correctly, the packet contains the server's public IP and not its private IP. Therefore, when this packet arrives at the NAT router, the router has no way to tell which private IP address to use.

**28. What is the difficulty with running a peer-to-peer application behind a NAT router?**

Generally, a peer machine both establishes and listens for new TCP connections (in a manner of speaking, it acts as both a client and a server at different times). Since all peers need to receive incoming connections, they experience the same problem as the server discussed in the previous question.

**Reading - BGP Routing Policy in ISP Networks**

**29. Why is BGP considered an incremental protocol?**

BGP only transmits its entire routing table when neighbors make initial contact. Afterward, only changes to this information are exchanged between neighbors. Therefore the routing tables are maintained via incremental updates.

**30. What does it mean for an attribute in the BGP decision process to be set by policy? Give an example of how a route can be determined by policy.**

Routes between neighboring ASes may be more desirable for economic, political, security or scalability purposes even if they have undesirable attributes like a longer AS-Path length. Policy attributes like Local Preference, Multiple Exit Discriminator, enable network operators to configure their networks to reflect these purposes.

For example, a network operator can set the Local Preference value such that a route to a destination AS is chosen from multiple candidate routes based on which route is the most profitable, rather than which route is the shortest.

**31. Describe how an AS can set import filtering policies to protect itself from falsified BGP updates.**

Import filtering can be used to eliminate bogus route advertisements that advertise routes to or through special use and private addresses, or routes to addresses not owned by the advertising AS.

Additionally import filtering can be used to ignore DoS attacks using BGP route updates. This is accomplished by setting the import filtering policies to ignore updates from offending addresses.

## Router Design Basics

**32. Describe the basic functions any router on the Internet must be able to perform in order to route traffic. What are some of the hardware features present on modern routers that support these functions?**

A router on the Internet at minimum must:

a. Receive packets
b. Determine destination of the packet
c. Create and maintain a packet forwarding table
d. Modify the packet as needed
e. Forward the packet.

Routers include hardware support including but not limited to the following that support these basic tasks:

1. Internal memory on each line card supports distributing copies of the forwarding table, eliminating a forwarding bottleneck.
2. The interconnection fabric features a crossbar switch that connects each input port to every output port, maximizing forwarding efficiency with parallelization.
3. The interconnection fabric hardware often has greater bandwidth than the line cards themselves (Speedup), preventing traffic from waiting in output queues.
4. Internal memory on each input port supports queuing (including virtual output queues) at the interconnection fabric, preventing data from being lost due to scheduling "collisions".

**33. Describe the purpose of a Maximal Matching switching algorithm commonly used to schedule traffic on router crossbars.**

The maximal matching algorithm permits maximum possible forwarding efficiency with-in a router's interconnection fabric. Given a list of traffic forwarding demands as input, it outputs a one to one mapping of input ports to output ports, such that no additional forwarding demands from the input list can be added to the mapping that increases the number of forwarding demands serviced during the single timeslot. Stated another way, the output of the maximal matching algorithm is a subset of (or equal to) the forwarding demands that represents the most effective use of the interconnection fabric.

**34. How would a router schedule bandwidth for a single timeslot (1s) for the following forwarding demands using a Max-Min Fairness algorithm (in Mb): 1.8, 2.4, 3.0, 5.3, 6.4, 1.0, 2.2, 8.0? Assume the algorithm can forward at most 25.6 Mb of data in a single timeslot.**

The total bandwidth available is first fairly distributed across all eight demands. Each demand is allocated 3.2 Mb. This satisfies demands 1, 2, 3, 6 and 7. Excess allocation is "reclaimed" from each of

these demands: 1.4 Mb from demand 1, 0.8 Mb from demand 2, 0.2 Mb from demand 3, 2.2 Mb from demand 6, and 1.0 Mb from demand 7, totaling 5.6 Mb.

Redistributing this available allocation over the remaining unmet demands, demands 4,5, and 8 are each allocated an additional 1.87 Mb (5.6/3). Added to the originally allocated 3.2 Mb, each of these demands now has 5.07 Mb of bandwidth. Because this satisfies none of the remaining demands, the final Max-Min fair allocation is [1.8, 2.4, 3.0, 5.07, 5.07, 1.0, 2.2, 5.07].

**Reading – An Update on IPv6**

### 35. Why has deployment of IPv6 been slow to gain momentum despite the exhaustion of IPv4 address space?

There are many reasons explored in the presentation:

1. IPv6 does not offer any distinct advantages over IPv4, it only provides additional address space. This means adopting IPv6 does not provide any "bang for the buck" and economic motivation for migrating to IPv6 will be driven by scarcity of IPv4 space, not by benefits of IPv6.
2. Network Address Translation (NAT) has been effective at expanding the IP space, particularly in in residential sectors. This means it is still possible to continue using IPv4 without serious consequences for a large number of users of the Internet, despite the fact they have many devices demanding access.
3. Group mentality - Many organizations are waiting for adoption rates to increase before migrating to IPv6, resulting in a waiting game.