Network Pre-Reading

The objective of this reading is to ensure that your knowledge of basic Internet network protocols is sufficient to support the study of network security issues, attacks, and controls.

The content of this note is not tutorial; rather it briefly summarises important concepts, together with indicative reading for students who find any of the material unfamiliar.

This document is organised as follows: Section 1 describes reference material, both recommended reading sources and definitive standards. Section 2 describes network architecture aspects such as layering. Subsequent sections describe the network layers in turn, starting with the link level, through the network layer, and finally describing important transport protocols.

Both IPv4 and IPv6 are included here; at present IPv4 is still the most prevalent protocol and will be used for most of the examples in class; IPv6 material is included for information and completeness.

How to use this document:

Read this carefully. Important terms that will be used in class are highlighted in **bold**; if any of these are unfamiliar then ensure that your reading covers these points. The cited reading material (section 1) provides possible sources of information; there are many other on-line sources that can be researched, depending on your existing level of knowledge.

Each section includes one or more questions. They generally require straightforward answers; however, answering these questions will require reading beyond these notes, and will consolidate your understanding of the material summarised here. **Please bring your answers to the NTAC (Network and Communications Security) module for discussion**.

If there are any questions about the scope or depth of the required reading (or other aspects of this), please contact Radu. **Email: radu.calinescu@york.ac.uk**

Contents

1. Reference Material

1.1. Recommended Sources

The following books provide a comprehensive introduction to networks and protocols; their authority, quality of explanation, coverage, and depth is significantly better than most on-line tutorial resources.

All three sources cover the basic protocol material identified in this note, with the exception of some specific material (e.g. Wi-Fi) where supplementary material is suggested below.

TCP/IP Illustrated, Volume 1

Kevin R.Fall, and W.Richard Stevens, *TCP/IP Illustrated, Volume 1*. 2nd edition. Professional Computing Series. 2012: Addison-Wesley. ISBN-13:

> This book is focussed on how current Internet-based networks work. It is a detailed core reference book for professional network engineers. It is accessible to those with less knowledge; however, the level of detail may obscure some of the fundamentals for those with no previous background in networks.

TCP/IP Tutorial and Technical Overview

Parziale, L., et al., *TCP/IP Tutorial and Technical Overview*. 2006, IBM International Technical Support Organization. Available at: http://www.redbooks.ibm.com/redbooks/pdfs/gg243376.pdf

> This provides a comprehensive reference to protocols and associated standards. The descriptions are a little more compact than the above book, so it may be less accessible to students with no prior knowledge of networks. However, this is a worthwhile download for its detailed referencing of relevant standards.

Computer Networks

Andrew S. Tanenbaum, and David J. Wetherall, *Computer Networks*. 5th edition. 2010: Prentice Hall. ISBN-13: 978-0132126953

> This book provides a wide perspective on networks, both by explaining network design choices and tradeoffs, and by describing non-Internet networks such as telephone systems. It is helpful in providing background material for those with restricted prior knowledge of the subject and provides sufficient information on basic protocols for pre-reading. It is not a detailed protocol reference.

1.2. Supplementary Material

The following additional sources are suggested:

802.11 – Frames and open authentication, available at https://supportforums.cisco.com/docs/DOC-24651

> Describes Wi-Fi management frames and how wireless connections are established.

Iljitsch van Beijnum, *IPv6 Internals*, The Internet Protocol Journal, vol 9 no 3. available at http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_9-3/ipv6_internals.html

> An accessible summary of the primary features of IPv6.

1.3. Standards and Reference Material

These references are provided for completeness, detailed knowledge of the relevant standards is not essential for the Cyber Security MSc.

Internet Engineering Taskforce RFCs

Internet Protocols are specified in *Request For Comments* (RFCs) by the Internet Engineering Task Force. RFCs include both standards and relatively informal documents, such as the short tutorial on TCP/IP (RFC 1180) and the *Security Glossary* (RFC 2828). They can be accessed online at:

http://www.rfc-editor.org/index.html

Institute of Electrical and Electronics Engineers (IEEE)

IEEE standards specify the physical layer of many types of network. In particular, the 802 series of network standards include both Ethernet (802.3) and Wireless (802.11). The 802 series standards are available for free download at:

http://standards.ieee.org/about/get/

IEEE standards are not generally available free on-line; the standards are published at:

http://standards.ieee.org/findstds/index.html

Organization for the Advancement of Structured Information Standards (OASIS)

This organisation issues standards prefixed with 'OASIS'; those of particular interest cover web-services protocols and security. They are available on-line at:

https://www.oasis-open.org/standards

Federal Information Processing Standards Publications (FIPS)

The FIPS series of standards include specifications for cryptographic algorithms and hashes. They are available online at:

http://www.itl.nist.gov/fipspubs/

The National Institute of Standards, Computer Security Resource Center

NIST publish a 'special publications' series, referenced with the prefix 'SP 800-'. These are not standards, but they provide a rich source of authoritative guidance and good practice for computer and network security. Publications are available on-line at:

http://csrc.nist.gov/publications/PubsSPs.html

2. Network Concepts and Architecture

A **protocol** is: *a set of rules (i.e., formats and procedures) to implement and control some type of association (e.g., communication) between systems. [RFC 2828]*. In general, for each protocol we need to understand the order in which messages are exchanged, and their content.

Using Internet terminology, communications takes place by exchanging **Protocol Data Units** (PDUs) between **peers** across the network, for example between a browser and a web-server. Most **PDU**s are structured, containing a **header**, a **body**, and sometimes a **footer**. Communication between peers is facilitated by lower-level network components that actually move the data across the network. This results in a **layered** network, in which each layer has a particular function. The implementation of these layers is often called a *network stack*.

The TCP/IP layered model (or ARPANET model) has 4 layers:

Application:	provides primary computing functions, usually for a user.
Transport:	implements the movement of data between applications, usually ensuring some degree of reliability.
Network:	moves data efficiently across networks between end-systems.
Link:	moves data between two devices, for example over a physical connection.

In practice the layers are often subdivided, particularly where it is necessary to add security features such as encryption. For example, a *Network Adjunct* layer between the Network and Transport layers is used to support IPSec.

The TCP/IP reference module is now dominant in practice; another model often referenced in network literature is the *OSI reference model*. This has 7 layers, with two specialised layers (*Session* and *Presentation*) between Transport and Application.

Each layer receives **Service Data Units** (SDUs) from the layer above, which are the PDUs which the higher layer is attempting to exchange with its peer across the network. After processing (e.g. *fragmentation*), data from the higher layer is **encapsulated** in the body of the PDUs of the lower layer, and headers and footers added to facilitate the lower-layer's protocol with its peer.

Network components may be characterised by the **layer** to which they operate. For example a router is a **network device**, which means that it will interpret the headers of network layer PDUs (IP datagrams, aka packets), but not interpret protocols contained within the body of these packets.

Question

1. Consider a network with two application-level endpoints communicating through a single network-level router. Draw a diagram of the network stacks in the three devices, and show all the peer-to-peer relationships between the layers.

3. The Link layer

The purpose of the link layer is to carry IP packets over physical media (wire, wireless), and support protocols related to the management and addressing of the link layer. The most common types of link layer are **Ethernet** and **Wi-Fi**, both defined in IEEE 802 standards which specify both the physical characteristics of the media used to carry data, and the associated protocol.

3.1. Ethernet

The original Ethernet design allowed a number of **Network Interface Cards** (NICs) to be connected to the same physical wire. The connection was shared using a technique called *Carrier Sense Multiple Access with Collision Detection (CSMA/CD)*. Essentially, if two devices connected to the wire attempted to transmit at the same time, they would detect the collision, broadcast a jamming carrier, then each would stop and wait a random interval before retrying. Current Ethernets use the same protocol, but have replaced a shared wire with a switched infrastructure (see 3.4).

Each NIC has a **Media Access Control Address** (MAC Address), which is a unique identifier in that physical segment. The MAC address is usually printed as six hexadecimal bytes in transmission order. (e.g. 00:23:AC:00:01:BF) of which the first three octets (e.g. 00:23:AC) are usually an *Organisationally Unique Identifier* (OUI) which specifies the organisation[1] that manufactured the NIC (e.g. CISCO) and may therefore suggest the type of the device. Special reserved MAC addresses are used to designate **multicast** and **broadcast** addressees.

Data are carried across an Ethernet connection in an **Ethernet Frame** which begins with a preamble and start of frame marker to allow the transmission to be synchronised, and concludes with a **Cyclic Redundancy Code** (CRC) to allow error checking. The body of the frame includes MAC source and destination addresses, an **EtherType** protocol identifier field, an optional *802.q tag* field, and the frame **payload**.

IEEE 802.q specifies how *Virtual Local Area Networks (VLANS)* are implemented, note that Ethernet VLANs are not implemented by encapsulation (i.e. a frame is not the payload of a frame) but by the addition of an optional tag within the frame: an *802.q header field*.

Questions

2. How does a NIC detect if an Ethernet frame contains an IP packet?

3.2. Wi-Fi[2]

Wi-Fi is a generic name for radio data systems implementing standards in the *IEE 802.11* series. The physical device that communicates over wireless is known as a **Station** (STA); the term *Wireless Network Interface Card* (WNIC) is also used. Some stations provide **Access Points** (AP) to a wired infrastructure known as a **Distribution Service** (DS), which may include access to the Internet. A single access point, together with the stations it supports, is known as a **Basic Service Set (BSS)** in which the access point is identified by a **Basic Service Set Identifier** (BSSID), essentially a MAC address of the access point. A group of BSSs that together form a wireless local network and facilitate roaming is known as an **Extended Service Set**, and is identified by a single **Service Set Identifier** (SSID).

The management of Wi-Fi packet transmission is conceptually similar to Ethernet: a protocol known as the *Distributed Co-ordinating Function* (DCF) detects if other stations are transmitting frames and implements an avoidance/backoff algorithm. The available radio spectrum is divided into a small number of **channels**, which can be used independently. Within each channel a complex form of radio modulation is used to optimise reception and bit-rate.

---

[1] http://standards.ieee.org/develop/regauth/oui/oui.txt

[2] An introduction to wireless protocols can be found at: http://technet.microsoft.com/en-us/library/cc757419(v=WS.10).aspx

A Wi-Fi frame has a preamble and physical layer header, followed by the MAC PDU; the normal format of an 802.11 MAC PDU is a header, payload, and a *Frame Check Sequence* (FCS) which is a CRC. At the start of the header a **Frame Control Field** specifies important attributes of the frame, including the **Frame Type**, which may be *Data*, *Management*, or *Control*.

The 802.11MAC header includes up to 4 MAC addresses, the meaning of which are determined by two flags in the frame control header: **To Distribution System** (ToDS) and **From Distribution System** (FromDS). Access points relay packets into a wired network, so in addition to the MAC addresses of the sending and receiving access points it is necessary to include a third address: the address to which the access point should forward the payload (ToDS via Ethernet) or the address from which the packet has been forwarded (FromDS). It is possible for ToDS and FromDS to be set simultaneously, which means that the packet is between two access points that are being used to connect two different wired infrastructures: this is known as a *Wireless Distribution System* (WDS).

The **Data Frame** encapsulates a protocol packet (such as IP) in its payload field. However, the encapsulation is not quite consistent with Ethernet; most of the logical link control information (e.g. addressing) found in an Ethernet header is contained within the 802.11 (Wi-Fi) MAC header; however, the 802.11 payload includes an 8 byte header before the encapsulated data. The last two bytes of this payload header are the **EtherType** field.

Control Frames are used to synchronise the transmission of data between two stations, and are simple MAC frames with no payload and only two addresses (receive/transmit station MACs). The frame types are determined by flags in the frame control field, and implement a standard modem protocol: Ready to Send (RTS) - Clear to Send (CTS) – [data] – Acknowledge (ACK).

Management Frames[3] are used by mobile stations to locate access points, authenticate stations and associate stations with access points. Access points are located by monitoring BSS **Beacon** frames transmitted by access points, or by a mobile station sending a **Probe** containing an SSID and receiving a **Response** from available access points. *Authentication* frames support an authentication message exchange; however, the actual flow of messages and frame content depends on the type of authentication. Following authentication, an **Association Request** allows a mobile station to request an association with an access point, and the requested association is confirmed or refused by an **Association Response**. Stations may ask to move between access points by using a **Reassociation Request,** or terminate an association with a **Disassociation** management frame.

Questions

3. You observe a Wi-Fi data frame with the following flags: FromDis - not set; ToDis – set. What types of station are the source and destination of this frame, and what addresses are present in the frame?

3.3. Link Layer Address Discovery

3.3.1. Address Resolution Protocol (ARP)

Network layer endpoints are known by their IP address, while at the link layer the associated NICs are known by physical MAC addresses. **ARP** is a protocol which allows an endpoint to discover the MAC address of a NIC from its IPv4 address.

An endpoint wishing to identify a MAC address broadcasts an Ethernet ARP frame to every host on the network segment; if a host is configured with the IP address specified in the request it sends an ARP response to the originator.

Hosts and network components usually cache ARP replies in a lookup table with a default lifetime of 20 minutes [RCF1122].

[33] Not covered in detail in the source books, online alternatives include *802.11 – Frames and open authentication*, available at https://supportforums.cisco.com/docs/DOC-24651

3.3.2. Address Resolution in IPv6

Address resolution in IPv6 uses the **ICMPv6 protocol** (see 4.4); the request is known as a *Neighbour Solicitation*, and the response a *Neighbour Advertisement*. Instead of a broadcast address, a *Solicited Node Multicast* address is used.

Questions

4. What is the destination address of an ARP request?

3.4. Link Layer Components

The link layer often uses components that extend the range or connectivity of the physical transmission media; examples are wireless *Repeaters* and network *Hubs*. An Ethernet hub simply copies every incoming packet to every port. A more efficient solution is to use a *bridge*, usually known as an Ethernet **Switch** to link together different parts of the same network segment. In modern networks it is usual for every endpoint in the network to be connected directly to a switch and this arrangement has replaced the 'shared wire' of the original Ethernet.

A switch 'learns' where to send frames by observing MAC addresses that appear as source addresses in the packets it receives, these are recorded in an internal **switch table** (called by many names, including *Hash Table* or a *CAM* - content addressable memory) which maps MAC addresses to switch ports. Frames with mapped MAC addresses are sent only to the associated port.

Some switches are configurable, allowing MAC addresses to be restricted to particular ports, or to provide *spanning ports* to which all traffic is directed regardless of the mapping.

Switch fabrics can become sufficiently complex to allow the possibility of multiple paths to the same endpoint. In such a fabric a distributed algorithm known as *Spanning Tree Protocol* is used; a root node is selected then each switch measures its distance to the root (actually a cost function rather than a simple hop count); only the lowest cost routes are enabled.

Questions

5. You connect a network monitor to a normally configured switch port in the hope of observing traffic between two network endpoints that are connected to the same switch. What traffic do you observe?

4. The Network Layer

The network layer moves **datagrams** (aka *packets*) between network end-points, its primary function is routing – deciding where to move each packet - and it is optimised for performance and simplicity rather than reliability. Packets that overload router bandwidth, become lost, or are corrupt are simply discarded.

Important features of this layer are the IP protocol including the structure and content of IP datagrams, and how IP addresses are assigned, managed and discovered.

Closely related to IP is the *Internet Control Message Protocol* (ICMP) and the *Domain Name Server* (DNS) protocol. Strictly these are both higher layer protocols; they are included here because of the key part they play in managing the Network layer.

4.1. The Internet Protocol (IP)

There are two sets of IP standards: **IPv4**, which is the most prevalent, and **IPv6** to which the Internet is in slow transition. IPv6 was motivated by the need for a larger address space (128 bits, as opposed to 32 bits), and includes other rationalisations.

A precursor to understanding IP packets 'on the wire' is an understanding of the order in which data are transmitted: **Network Byte Order**. Fields within an IP header are transmitted in order, and within each field the bytes are transmitted in descending order of significance (most significant byte transmitted first), also known as *Big Endian*[4].

A standard IPv4 datagram comprises a header followed by a payload; the normal header size being 20 bytes. The fields in an IPv4 header include: **Total Length, Time to Live, Protocol, Header Checksum, Source IPv4 Address** and **Destination IPv4 Address**. IPv4 headers may be extended by options, although the use of such options is relatively rare in current networks.

IPv4 and IPv6 datagrams are distinguished apart by the header **Version** field.

IPv6 headers are fixed at 40 bytes and have a simpler structure than IPv4, reflecting a focus on information that is used for routing. IP header information that is primarily used by end-systems (e.g. security data) is supplied in *Extension Headers*, as indicated by a *Next Header* field. Fields in IPv6 include *Payload length*, *Hop Limit*, *Source IPv6 Address* and *Destination IPv6 Address*.

Questions

6. What purpose does the IPv4 'Time to Live' value serve?
7. What is the scope of the IP Header Checksum (i.e. what does it check)?

4.2. IP Addressing

4.2.1. Addresses

IPv4 addresses (32 bits) are normally written in **Dotted Decimal** notation (e.g. 192.168.0.1) with the most significant byte first. IPv6 addresses (128 bits) are normally written as eight blocks of 4 hexadecimal characters, together with shortened forms that omit leading zeros or all zero blocks [RFC4291] (e.g. 7f01:5a::80).

IP addresses are assigned hierarchically, using a scheme known as **Classless Inter-Domain Routing** (CIDR); essentially a number of bits (starting from the most significant bit) are assigned as a **Network Prefix**, and the remaining bits of the address are assigned by the authority who has been granted that prefix. A similar scheme is used within local networks, where the prefix defines the address space of a **Subnet**. The Number of bits in the prefix are specified by a **Mask** (either a *CIDR Mask* or a *Subnet Mask*) which is usually indicated by a '/' (e.g. 192.168.0.0/24 specifies that 24 bits – the first three bytes – is the address of this subnet and the remaining byte can be allocated locally).

[4] Within computers data are usually stored in *Little Endian* order: least significant byte first. This distinction is an issue only when viewing the raw data of network packets within computer memory or disk.

Both IPv4 and IPv6 include **Reserved or Special-Use Addresses** [RFC 5735 and RFC5156 respectively], for non-routable, multicast and broadcast addresses. Non-routable addresses are used for private networks (e.g. 192.168.0.0).

In IPv6 an address prefix signifies its **scope** – e.g. **link-local** (the local subnet) or **global**. Unlike IPv4, IPv6 does not include a reserved address for broadcast; instead, reserved multicast addresses are used.

The 64 least significant bits of a unicast IPv6 address is an *Interface Identifier*, which is usually the MAC address of the associated NIC, or may be a random number intended to provide some degree of 'privacy' (address anonymity).

IPv6 Interfaces support a number of IP addresses rather than a single address; most interfaces will at least support a link-local address and a global address.

Questions

8. What IPv4 address is used to broadcast to the local network?
9. What is 10.0.0.0/8?
10. What is the full hexadecimal IPv6 address of 7f01:5a::80?
11. What is fe80::/10 ?

4.2.2. Address Allocation

Public IP addresses are assigned hierarchically; the primary authority being the *Internet Corporation for Assigned Names and Numbers (ICANN)*, which delegates subsets of the available address space to **Regional Internet Registries** (RIRs), who in turn delegate address space to smaller registries, or to larger *Internet Service Providers* (ISPs). The registries provide query services to identify who is responsible for particular address allocations[5].

Network Address Translation is used at the boundary of a network, allowing a small number of assigned IPv4 addresses to be shared between hosts on a local network. The local network hosts use a larger pool of non-routable addresses. NAT rewrites the source/destination addresses of IP datagrams as they transit a router. The most common algorithm is **Network Address Port Translation**, which uses transport-layer ports to differentiate internal hosts.

Nat will probably not be used for IPv6, although it has some potential for gateway management.

Dynamic Host Configuration Protocol v4 (DHCPv4) is used to assign local IPv4 addresses from an **Address Pool**, and to provide other configuration information such as the subnet mask, the addresses of a Default Router (see 4.5.1), and a DNS server address (see 4.3.2). It is used extensively for automatic network configuration.

When a client requests an address the DHCP server allocates an IP address with a time-limited **Lease,** or a fixed pre-assigned address (usually for servers).

IPv6 takes the concept of a time-limited lease a stage further, applying it to all IPv6 addresses. IPv6 addresses have a specified *address lifecycle*. When they are first allocated they are tentative, until *Duplicate Address Resolution* confirms that they are unique, after which they become *Preferred*. Addresses have a *Preferred Lifetime* after which they become *Depreciated*, finally becoming invalid at the end of their *Valid Lifetime*.

DHCPv6 provides similar services to DHCPv4: the allocation of IP addresses and other configuration information. It operates in conjunction with *ICMPv6 Router Advertisement* messages, which are multicast periodically or sent in response to *ICMPv6 Router Solicit* requests. The Router Advertisement specifies if DHCP will be used for address and/or non-address configuration information, and usually the prefix(es) used by the subnet.

DHCPv6 servers are discovered by a *Solicit*/*Advertise* message exchange, after which a *Request*/*Reply* exchange is conducted to obtain information from the selected server. Because interfaces have several

[5] The European registry may be queried via https:/apps.db.ripe.net/search/query.html

IPv6 addresses, clients requesting address allocation from a DHCPv6 server identify themselves with a persistent *DHCP Unique Identifier* (DUID)

Questions

12. Use the RIPE registry to determine the organisation and network name associated with 144.32.128.73 and the address range of which it is a part.
13. How is a NAT and local DHCP configured to allow access from the Internet to an internal web server?

4.3. IP Address Discovery

4.3.1. The Domain Name Space

To provide 'human friendly' names for Internet end points, and to allow some flexibility of IP address assignment, **host names** are used to identify Internet end systems. The names are assigned hierarchically, the root authority being the *Internet Corporation for Assigned Names and Numbers* (ICANN). At the highest level of naming are **Top Level Domains** (e.g. .com, .uk) each of which is managed by a registrar. Note that domain names can be extended inside organisations (e.g. cs.york.ac.uk) to identify organisational units.

Every domain has a number of associated **Resource Records**, which include host addresses for a Name Server (**NS**), Mail exchange (**MX**) and IP address ('**A**' for IPv4, 'AAAA' for IPv6)

4.3.2. Domain Name Resolution: Domain Name Server (DNS)

The DNS protocol is used to obtain resource records from a Domain Name Server. The most common use of DNS is to obtain an 'A' record: i.e. to look up an IP address given a name.

Domains are grouped into **Zones**, each of which has a **Name Server**. Zones are hierarchically structured and the closest name server to a host holds an **authoritative record** for that host. Other name servers in the Internet may hold **cached** records. At the top of the name server hierarchy are **root name servers**, which are used to identify **top level name servers** which contain resource records for the top-level domains. Usually, a request to a name server for a host record that is not cached results in a sequence of requests down the hierarchy to obtain the address of the server with an authoritative record. This name server is then queried for the required host IP address, and this result is then cached for future reference.

Questions

14. Your host, H, is within the A.GOV domain. What set of DNS queries take place when you attempt to access http://www.myinc.com / ? (Assume that no cached records are in place.)

4.4. Internet Control Message Protocol (ICMP)

ICMP (v4 and v6) is a protocol that operates above the IP layer, but does not make use of the transport layer; it has its own *protocol identifier* in IP datagrams. The protocol provides a range of information and error messages that assist the management of an IP network. The most frequent messages encountered are **Echo** and the **Echo Reply** response (usually known as *Ping*) which are used to check network connectivity, and the error messages *Destination Unreachable* and *Time Exceeded*. The last of these is used in the important debugging tool **traceroute**.

ICMPv6 carries out similar functions using different formatted messages, it is also used for neighbour discovery (in place of ARP) and router discovery.

Questions

15. There are two routers between your end system and host X: *Router A*, then *Router B*. What sequence of datagrams do you observe at your system as a result of running traceroute with X as the target?

4.5. Network Layer Components

4.5.1. Router

A **Router** is a Layer 3 device which joins two networks. Its primary function is to forward IP datagrams on a hop-by-hop basis; when it receives a datagram it uses a **routing table** to identify the correct link (interface, MAC address or other link level identifier) on which to output the datagram. Routers use a *longest prefix match* algorithm to select the best matching table entry for a particular destination IP address. Packets that fail to match any entries are discarded and may result in an ICMP error message.

A very common entry in a routing table is a **default route** (in local networks sometimes called *default gateway*): where to send packets that match no other entries in the router table. In some routers (e.g. local network gateways) this may be the only entry in the table.

4.5.2. Gateway

Gateway is a general term for a device that joins two systems, often with disparate protocols and identified with a particular layer. For example an *Application Gateway* might carry out protocol translation between different email systems. The term *Network Gateway* was originally used for what is now known as a router.

In current usage a device which acts as an Internet endpoint and hosts a private network is often known as a Gateway. Such gateways provide router functions, and often a range of other services at different layers, including NAT, DHCP, DNS and the termination of Virtual Private Networks (VPNs).

Questions

16. A router table has entries for 230.0.0.0/8, 230.13.1.0/28 and a default route. Which entry matches the destination address 230.13.0.1?
17. A host wishing to send an IPv4 packet to an IP address for the first time checks if the address is in the same subnet, or a different subnet. What is its next action if the IP address is in (a) the same subnet, or (b) a different subnet?

5. The Transport Layer

The transport layer provides some degree of reliability of data transmission between two endpoints, and it extends the addressing of messages to services within a host.

5.1. Ports and Services

IP addresses generally represent physical hosts; the transport layer extends the IP address with a finer grain abstract address known as a **Port**. Generally the end-point of a transport protocol is known as a **Socket**, the address of which is a combination of the IP address of the endpoint, and the port number. Particular ports may be associated with particular services or applications; **Well-Known Ports** are standard addresses for specific Internet protocols, and are assigned by the *Internet Assigned Numbers Authority* (IANA)[6].

Questions

18. What transport protocols and ports are used for: DNS, and Web Servers (HTTP)?

5.2. User Datagram Protocol (UDP)

A **UDP datagram** is a short message which can usually fit into a single IP packet. The UDP protocol is a lightweight connectionless protocol that simply attempts to deliver UDP datagrams to a destination address and port. No guarantees are made of the completeness of a sequence of datagrams, or their arrival order; however, the protocol does provide a datagram checksum, and a port address.

5.3. Transmission Control Protocol (TCP)

The TCP protocol provides a reliable end-to-end 'connection', or byte stream, between two endpoint ports. Byte streams presented to the TCP protocol are packaged together with TCP protocol headers into **TCP Segments**, each of which can be accommodated within an IP packet. The operation of TCP is adaptive to network conditions, based on a core protocol known as the *Sliding Window Protocol*: a sender retransmits a segment if an acknowledgement is not received by the end of the window timeout.

The protocol header in a TCP segment includes a number of flags (ACK, SYN, FIN, RST) which are used in data transfer control, and also in the process of establishing and closing a connection. The usual connection establishment process is a **three way handshake** (client request - server acknowledgement – client acknowledgement). This identifies the requested port and establishes *sequence numbers* used in the sliding window protocol.

Questions

19. What flags are set during the three way TCP establishment handshake?
20. A server responds to a client connection request with a RST flag; what does this signify?

[6] See http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xml