Lecture Notes

Introduction to Digital Networks and Security

Raj Bridgelall, PhD

Table of Contents

Networking Concepts

1 Introduction

This lecture note summarizes numerous network communications concepts that are needed to appreciate various topics in cybersecurity.

2 Data Communications

The transmission of data between applications on remote computing nodes involves a well-defined process for generating data packets and eventually converting them into transmissible bit streams for reliable end-to-end delivery over an unreliable and untrustworthy media.

2.1 The OSI Model

Classical network communications theories layer each of these well-defined processes into a stack consisting of seven layers. The International Standards Organization (ISO) created a broad set of specifications for these seven layers. The ISO organized them into a model called the Open Systems Interconnection (OSI) to facilitate widespread and standardized development of interactive systems for a public network such as the Internet. These seven layers, starting with the one closest to the hardware level are the physical, data link, network, transport, session, presentation, and application layers (Forouzan 2012).

A	Application – serves as the interface for users and application processes that need access to network services. Involves resource sharing, remote file access, remote device access, directory services, and network management.
P	Presentation – formats the data for presentation to the application layer. Involves character and syntax translation, data compression, encryption, and decryption.
S	Session – establishes, synchronizes, maintains, and terminates communications sessions between nodes. Involves security and logging functions.
T	Transport – protocol that assures error-free delivery of the message, in the correct order, and without duplication. Involves message segmentation, acknowledgement, and multiplexing.
N	Network – **packet** assembly to control the subnet operations and routing of network traffic. Contains the Internet Protocol (IP) addresses of the source and destination nodes.
D	Data Link – **data frame** assembly and sequencing that establishes and terminates a reliable logical link between nodes. Contains the media access control (MAC) address of the node.
P	Physical – hardware and software involved with the transmission and reception of **binary digits (bits)** over the physical medium. Involves the data encoding and transmission methods.

Figure 1: The OSI Model.

The *physical layer* is responsible for the transmission of bits over a physical medium with pre-defined electrical and mechanical specifications. The bit encoding and bit representation schemes are also determined at this layer. For example, at this layer we consider the carrier modulation method and power fluctuations by which 'ones' and 'zeros' of a digital bit stream are represented for physical media transmission. IEEE 802.3 is an example of a physical layer specification that defines a bit encoding scheme (e.g. Manchester 10BaseT, 100BaseT, etc.) and a channel access mechanism based on Carrier Sense Multiple Access/Collision Detection (CSMA/CD.) Originally developed by Xerox Corporation and later extended as a joint venture that added Intel and Digital Equipment Corporations, the IEEE 802.3 specification, also called Ethernet, became the most popular physical layer specification for Local Area Network (LAN) communications.

The *data link layer* organizes bits into *frames* for node-to-node delivery. It adds *headers* and *trailers* that get the frame from one physical node to the next in an error free manner. With flow control, the data link protocol orders the frames and regulates the amount of data sent so as to prevent receiver overflows. Synchronization bits alert the receiver when frames begin and end and error bits indicate the need for re-transmission. Some examples of data link protocols are XMODEM, LAPD (used in ISDN), PPP (used for serial communications between personal computers and cellular phones), and Frame Relay (used for LANs.)

For WLAN, the IEEE further sub-divided the data link layer into the Logical Link Control (LLC) and Media Access Control (MAC) layers. These implement the node-to-node and media sharing mechanisms respectively. The IEEE standardized the LLC implementation across all WLAN networks but allowed for dedicated implementation of the MAC as it pertained to the particular communications device. The LLC also contains source and destination port numbers that identify the application end-points of the sending and receiving machines. The MAC layer resolves the contention for the shared media. It contains the frame synchronization, error, flow control flags, control specifications, and physical addresses necessary to move data between nodes.

The *network layer* is responsible for moving *packets* from source to destination nodes so as to provide internetworking. It fragments the original message (packet) from the transport layer into manageable pieces (frames) for final delivery and eventual re-assembly. *Routers* on the network contain routing tables that facilitate the best known virtual path between intermediate nodes that will eventually get the frame from the source address to the destination address. As frames move between network nodes on its way to the final destination, each node substitutes an intermediate *data-link* address header that moves the frame to the next node along the way. However, the source and destination addresses do not change as frames move between nodes. The network layer is also responsible for media sharing and channel-access so that multiple frames from different applications can simultaneously move across the same physical media.

The *transport layer* provides a reliable end-to-end message delivery by overseeing the error recovery and flow control processes. Unlike the network layer, the transport layer recognizes a relationship between the frames so that they can be re-assembled into the original cohesive message packet and delivered to the appropriate application. Since several applications may be running simultaneously, the transport layer is responsible for identifying *service points* (also known as port or socket addresses) and to deliver the message to the intended application. Some session messages may be too long for reliable transport layer re-assembly or too short for efficient use of the media. Therefore, the original session message is also appropriately segmented or

concatenated. Each message is sequenced so that they can be re-assembled in the original order with which they were transmitted. Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) are popular transport layer protocols. They are briefly described in Section 2.3.

The *session layer* is responsible for establishing, managing, and gracefully terminating communication sessions between two remote applications. It synchronizes the interaction between the two network entities so that processes can be reliably completed. For example, it utilizes session checkpoints so as to continue processes from where they were suspended as the lower levels recover from intermittent communications failure due to packet loss or packet latency from a noisy or congested network.

The *presentation layer* translates between native communication languages, provides data compression, and encryption for secure communications. Data translation provides a uniform interface for applications running on any platform.

The *application layer* software programs facilitate access to the network resources. Some examples are directory services, mail services, virtual terminals, and file management.

2.2 Networking Devices

The Internet is made up of a number of networking devices called Repeaters, Bridges, Routers, and Gateways. *Repeaters* operate at the physical layer and their purposes are to regenerate the bit-stream in order that packets can reliably travel large distances between nodes. A repeater is not necessarily an amplifier, although the signal strength is generally restored to its original level.

Bridges operate at both the physical and data link layers. They divide a large network into smaller sub-networks or combine smaller sub-networks of the same type into a larger network. Bridges contain a list of all the nodes connected to either side of it and so it can intelligently filter and forward packets to the intended recipients on either side.

Routers operate in the physical, data link, and network layers and they are needed to establish the best paths for packets to travel along the way from source to destination nodes. They gain knowledge about the network configuration and path characteristics from periodic communications with other Routers. Eventually, all Routers have knowledge about the network to which they are connected so that each can determine the best path for routing packets. Routers use specific protocols and 'routing tables' to determine the 'best' path to other nodes on the network. They also track and update a packet's lifetime and may eventually 'kill' a packet if it has not found its owner within a predetermined time period. This mechanism prevents network congestion when disabled nodes cause looping or bouncing because packets reach dead-ends.

Gateways can operate in all seven layers of the OSI model and convert between protocols so that data can move across different network types. Physically, a gateway is no more than additional software running on a Router.

2.3 TCP/IP

The Advanced Research Project Agency (ARPA), a U.S. Department of Defense arm, developed TCP/IP in 1969 for connecting computers in a large network called ARPANET – now known as the Internet. TCP/IP developed before the OSI standard and, therefore, does not exactly match the OSI model. TCP/IP combines the three top layers of the OSI model (application, presentation, and session) into a single application or *message* layer. TCP or UDP is defined for the transport or

Segment layer and IP is defined for the network or *Datagram* layer. The data link and physical layers are network dependent and consist of an organized pattern of *frames* and *bits* respectively.

IP alone is *unreliable* and *connectionless*. Unreliability means that IP does not provide error checking or datagram tracking. Reliability is nevertheless obtained when IP is paired with a reliable transport protocol such as TCP. *Connectionless* refers to the fact that no *virtual circuit* is established for the transmission of the entire message which consists of an ordered series of datagrams. Each datagram is separately transmitted and does not necessarily follow the same path. Unlike a connection-oriented service, the receiver is not alerted about the incoming message and it is not expected to acknowledge successful receipt of the entire message once it has been completely transmitted.

Each datagram consists of a 20 to 60 byte header and a data portion where the total datagram length does not exceed 65536 bytes. The header consists of information essential for its routing and delivery. For example, the header includes fields containing the source IP address, destination IP address, and datagram lifetime. There are also numerous other fields that relate to packet fragmentation, service class, reference protocol, routing, timing, management, and alignment controls. IP addresses of the present Internet version (IPv4) consist of four bytes that define a class type, network identification (NID), and host identification (HID.) At present, only the third of five address classes is available for use. The first two are already full. The fourth class is for multicasting and the fifth is reserved.

IP supports three additional sub-protocols known as Address Resolution Protocol (ARP), Reverse Address Resolution Protocol (RARP), and Internet Control Message Protocol (ICMP.) ARP is used to associate an IP address with the physical address of the device, which is usually the Network Interface Card (NIC) hard coded address. Hosts and Routers find the physical address associated with an IP address by broadcasting an ARP query packet to every node on its sub-network and receiving an answer only from the owner. RARP allows a host to determine its IP address when it knows only its physical address. The host broadcasts its physical address in an RARP request packet and receives its IP address only from the network node that knows it. ICMP allows the host to determine when an IP datagram is undeliverable.

Both TCP and UDP represent the transport layer portion of the protocol. TCP is *reliable* and *connection-oriented*. UDP is *unreliable* and *connectionless* and is thus simpler and faster. In particular, UDP does not perform error checks or wait for packet receipt acknowledgements. Hence, it is typically used for streaming and online games. In contrast with IP, both UDP and TCP connections are port-to-port, which provides host-to-host connectivity. The multi-tasking operating system of the host machine assigns a port to each active process. A port is generally a data buffer with which a process is associated. As such, UDP and TCP *segment* headers carry both the source and destination port addresses. Unlike UDP, TCP also contains identification and sequencing numbers so that the specific lost or damaged segment can be identified. TCP sets up an end-to-end virtual circuit for the entire duration of the segment transmission so that the end ports know to expect more datagrams and to check their sequencing. This virtual circuit session should not be confused with that of the session layer protocol, which is more concerned with the entire message exchange and not just the segment. TCP achieves reliability by adding header information that facilitates error detection, acknowledgements, and frame retransmission.

3 Mobile IP

Mobile IP is a standard proposed within the Internet Engineering Task Force (IETF) that will allow a mobile unit (MU) to have both a fixed *home address* and a *care-of address* that changes as the MU roams through different networks (Perkins 1997). In effect, remote applications will continue to transparently interact with the MU as it roams seamlessly across IP-based networks. The scope of this standard includes only packet switched connections based on IP.

Mobile IP requires the existence of a *home agent* network node. Whenever the MU is attached to a foreign network, it registers with a *foreign agent* of that network. Vendors generally implement Mobile IP in routers that can serve as both home and foreign agents. The foreign agent assigns a new care-of address to the MU. As the MU moves between networks, it obtains a new care-of address via Dynamic Host Control Protocol (DHCP) and *registers* the new address with the home agent. Registration is done either directly or indirectly via the foreign agent, depending on the nature of the attachment. Mobile IP utilizes the User Datagram Protocol (UDP) with re-transmission parameters in order to avoid the complexities of Transmission Control Protocol (TCP.) After registration, all packets arriving at the home agent will be re-directed to the foreign agent at the care-of address. After receiving the re-directed packets, the foreign agent substitutes the destination-IP address for the static home-IP address and delivers the packet to the MU.

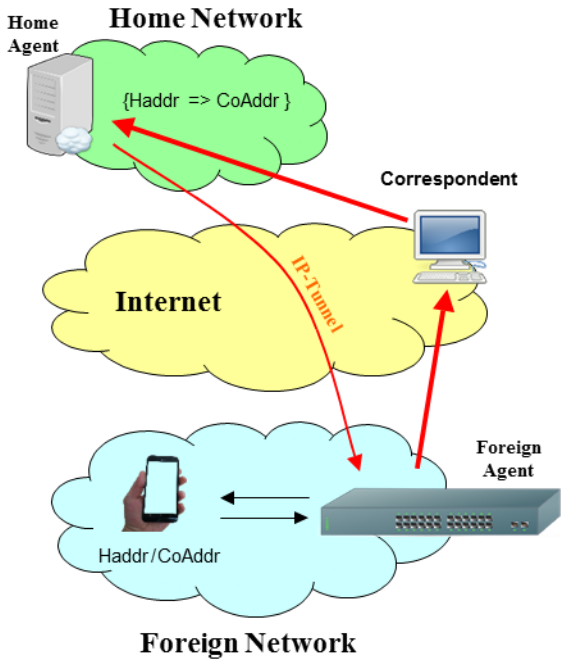

Figure 2: Illustration of the Mobile IP Process.

Mobile IP is implemented at the network layer of the OSI model such that applications running above, such as TCP, will be unaware of roaming as the MU changes its point of attachment to the network. Applications will see the MU's static home-IP address as its source address when the MU is sending data and as the destination address when the MU is receiving data. Therefore, Mobile IP implementation results in seamless application connectivity as the MU roams and attaches to topologically new IP nodes.

The home agent facilitates this transparency by re-encapsulating the arriving packets with a new

IP address destination wrapper to the care-of address. The foreign agent then unwraps the packet before forwarding it to the MU. This re-encapsulation is also frequently a subset of some secure *tunneling* protocol, for example, IPsec. Therefore, Mobile IP can effectively accommodate a VPN style tunnel between the home agent and the foreign agent. A secure connection between the home and foreign agents is necessary in order to prevent rogue network entities from inconspicuously updating the home agent with a fake care-of address, thereby redirecting packets to an unintended destination.

When MUs roam, they must either *discover* home and foreign agents via their *advertisements*, or they must solicit prospective agents. Several MUs utilizing a foreign agent may share a single care-of address. This works because the home address for each MU will remain unique and unchanged during the tunneling transit between the home and foreign agents. Therefore, after "de-tunneling," each MU will get the packets destined for them. MUs capable of running the Mobile IP protocol can serve as their own foreign agent provided that they have access to a DHCP server for IP address assignment. In this case, the specifications refer to the care-of address as a *co-located* care-of address. When serving as its own foreign agent, the MU must additionally be capable of running the required tunneling protocol. Foreign agents may directly route packets from the MU to the remote host and bypass the home agent during the reverse trip as illustrated in Figure 2. Hosts that are capable of implementing a directory cache of care-of addresses and a tunneling protocol can bypass the home agent and communicate directly to the MU. This is desirable for reducing network traffic congestion to the home agent as well as a potentially inefficient route between the client and server.

Although Mobile IP is one of the leading proposals for seamless roaming of next generation mobile Internet applications, there are numerous disadvantages to using the standard. For example, if the point of MU attachment changes faster than the round trip time for a packet, then the foreign agent routers will not have time to update their routing tables and packets will be lost. The round trip time for packets moving across the Internet depends on network utilization, congestion, number of operational nodes, etc. Also, TCP timers, such as packet time-out and retransmission counts, are not adaptively reconfigurable and depend on the network connection. Therefore, switching between the data rates of a slower wireless connection such as a WWAN and a faster wireless connection such as a WLAN may result in an inefficient data communications link. As tunnel overhead and network related delays between the home and foreign agents change while the MU roams, remote applications may unnecessarily increase error and flow control handshakes, thereby exacerbating the problem.

3.1 Firewalls

Firewalls monitor incoming and outgoing network packets to block or allow traffic based on a set of defined rules. They prevent packets that appear to have emanated from a node within the Intranet from re-entering. In doing so, a firewall is attempting to filter out potentially malicious packets that are intended to spoof internal computers. Therefore, the MU may not be able to communicate with neighboring nodes within its domain if the home agent is located outside of this domain. One solution is to setup a reverse tunnel from the foreign agent back to the home agent, thereby bypassing the firewall function. However, this results in network routing inefficiencies that can possibly lead to network congestion.

3.2 DHCP and DNS

The Dynamic Host Control Protocol (DHCP) provides new network clients with an IP address, the Domain Name Server (DNS) address, domain names, default Router addresses, and other configuration information needed for communications on the network. The DNS facilitates a user-friendly method of naming hosts and provides the equivalent host name or IP address if given either. When a client attaches to a network, it sends out a DHCP request. One or more DHCP servers or agents hearing the message will formulate a service offer to the client via its MAC address and source port. The DHCP server will not commit the IP address until the client acknowledges the response. The DHCP assigns a lease time to the IP address it allocates to the client. Hereafter the client is expected to renew the lease when it is at 67% of the expiration time or risk losing the IP address while in the middle of an application.

In order to facilitate Mobile IP with conventional networks having DHCP and DNS servers, the MU must use its new DHCP-allocated IP address as a co-located care-of address and update the home agent. That is, the MU must now serve as its own foreign agent. However, the MU may also ignore the use of the DHCP-allocated IP address and utilize one from an advertising foreign agent instead.

For WLANs, the access point (AP) can be configured as a foreign agent that advertises its services to MUs as they associate. Therefore, the AP can assign the MU a care-of address. The AP can also forward DHCP requests for a home IP address. In this case, the DHCP will return a home IP address that is closely associated with a nearby home agent with which the MU can register.

Mobile IP must also facilitate the time latency required for authentication and network security. Without network authentication, the MU cannot determine which DHCP server response is authentic nor can a DHCP server trust the MU. For example, rouge MUs can issue multiple DHCP requests, each with an associated fake MAC address so as to deplete the pool of IP addresses that the server can issue. MUs can also register normally but then configure themselves as fake DHCP servers and take control of the network.

3.3 IPv6

The number of Internet nodes has historically doubled every year. Each active Internet node requires a separate and unique IP address. With the explosive growth of Internet users, the present pool of IP addresses defined by IPv4 is dwindling rapidly. The Internet Engineering Task Force (IETF) first proposed IPv6 in July 1994 in order to address this and other issues. IPv6 provides four times more address bits for a total length of 16 bytes rather than four bytes of the current IPv4 standard. This results in $2^{(128-32)} = 2^{96}$ times more IP addresses. This is enough IP address to cover nodes on every square inch of every planet in the solar system.

Each IPv6 datagram is composed of a payload that can be up to 65536 bytes and a fixed base header that is 40 bytes long. The payload itself consists of an optional extension header plus the data from upper layers. The 40 byte base header consists of a 16 byte source IP address and a 16 byte destination IP address plus other fields that are needed to route the datagram more efficiently than IPv4 through the Internet. Extension headers provide a facility for better source routing, fragmentation, authentication, and security.

IPv6 incorporates many of the general ideas of Mobile IP. It incorporates several new features that removes the need for a foreign agent while more naturally facilitating the presence of a home agent entity. The home agent and the MU cooperate via a registration process involving the care-of

address obtained from network *access points*. In IPv6, the MU has more responsibility for managing its own mobility. The MU is also now able to automatically configure its care-of address at the point of network attachment so that it contains the proper foreign network prefixes and is also more globally routable based on its location. As the MU moves, it directly supplies location information to its remote correspondents. The MU does so by using the IPv6 *destination* and *security options* located in the extension headers. For privacy reasons, the MU is not obligated to always communicate location information directly to its correspondents. Therefore, the MU must also communicate care-of address updates to the home agent, which must now also acknowledge receipt of the updates. IPv6 also has a new *home address option* that is generally included for communications between the MU and its correspondent. This informs correspondents that for mobile devices, they should consider sending packets to the home address rather than to the source IP address (care-of address) that they find within the fixed base header. This mechanism effectively resolves issues with firewall filtering.

The MU keeps track of its connectivity status through Neighbor Discovery and Network Unreachability Detection (NUD) protocols. Routers periodically send multicast advertisements and this is one mechanism by which the MU determines the status of its network connectivity. Routers advertise their services such as whether or not they can serve as a home agent. In order to facilitate smooth handoffs between points of network attachment, the MU sends a location update packet to the previous router in order to indicate that it has moved to a new care-of address. Subsequently, the MU sends a location update to the remote correspondent.

In IPv6, each node on the network will have a destination address cache that it is responsible for updating. This mechanism allows each node to process location updates from the MU and, thereby redirect correspondence to the new care-of address.

4 References

Forouzan, Behrouz A. 2012. *Data Communications and Networking.* 5th. McGraw-Hill Education.
Perkins, Charles E. 1997. *Mobile IP: Design Principles and Practices.* 1st. Prentice Hall.

5 List of Acronyms

Acronym	Meaning
802.11a	A section of the IEEE 802.11 standard that specifies WLAN networks for speeds up to 54 MBPS using OFDM for channel access and QPSK or QAM for carrier modulation. In general, the 802.11 standard specifies channel sharing via CSMA/CA mechanisms that are managed by the MAC.
802.11b	A section of the IEEE 802.11 standard that specifies WLAN networks for speeds up to 11 MBPS using DSSS for channel access and QPSK for carrier modulation.
API	Applications programmer interface.
CSMA/CA	Carrier sense multiple access/collision avoidance.
HTTP	Hypertext transfer protocol.
IP	Internetworking protocol.
IPsec	IP Security – a set of protocols for secure exchange of Internet packets.
ITU	International telecommunications union.
LLC	Logical link control – upper sublayer of the data link layer as defined by IEEE 802.2.
MAC	Media access control.
MSC	Mobile switching center.
NAS	Network Authentication Server
PHY	Physical (layer.)
PPP	Point to point protocol.
RADIUS	Remote Authentication Dial-In User Service.
RTP	Real-time protocol.
TCP	Transmission control protocol.
UDP	User datagram protocol.
VoIP	Voice-over-Internetworking protocol.
VPN	Virtual private network.
WLAN	Wireless local area network.
WWAN	Wireless wide area network.