

CSIS 625 Week 12

TCP/IP continued, Presentation Layer

Copyright 2001, 2002, 2003 – Daniel R. Oelke

For use by students of CSIS 625 for purposes of this class only.

I. Overview

A. TCP/IP continued

1. Transport Layer - UDP or TCP
2. DNS
3. Routing example
4. Private IP addresses

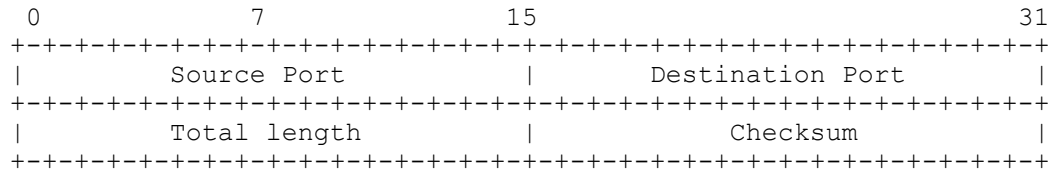
B. Presentation Layer

1. Network Management
2. Encryption – Symmetric and Public-Key
3. Authentication

II. TCP/IP

A. Transport layer – UDP/IP

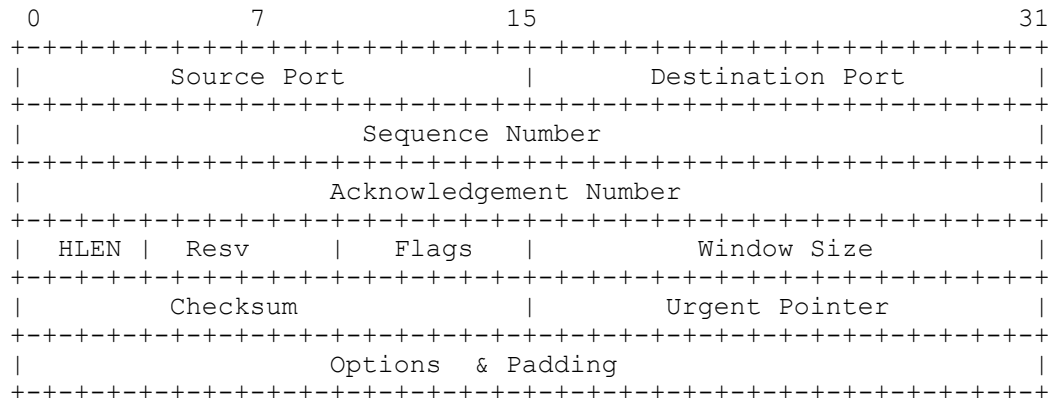
1. UDP is simple in that all it really has to support in addition to the IP header is port addresses.
2. Header format



3. Source and destination ports determine the service that is running them
4. Checksum protects the UDP header (not the packet data)

B. Transport layer – TCP/IP

1. TCP is connection oriented so it must provide connection setup and teardown as well as provide mechanisms for reliable packet delivery.
2. Header format



3. TCP Header

- a. Port Addresses – used to identify services

- b. Sequence Number & Acknowledgement number – used for sliding window flow control and error control
 - c. HLEN – Header length in multiples of 4
 - d. Resv – Reserved for future use
 - e. Flags –
 - (1) URG – Urgent – there is urgent data in the data portion
 - (2) ACK – The acknowledgement field is valid
 - (3) PSH – Push – higher throughput is desired
 - (4) RST –
 - (5) SYN – Sequence number synchronization in the connection setup
 - (6) FIN – connection termination
 - f. Window Size – The number of packets that can be sent.
 - g. Checksum – error detection for the header (not the data)
 - h. Urgent pointer – an offset into the data portion for where the urgent data is (if the URG flag is set).
4. TCP flow control
- a. TCP uses a modified sliding window technique - called a credit scheme
 - b. Each ACK has both a number in the window for the bytes that are being acknowledged, and a number in the window that may be sent up to before acknowledgement.
 - c. Slow Start - developed by Van Jacobson - 1988
 - (1) Exponentially increases the window size as data is successfully sent.
 - (2) Allows the amount of data being sent to grow up to the network capacity.
 - (3) Causes “slowness” for very short data transfers
 - d. Dynamic Window Sizing on Congestion
 - (1) When a packet is lost, and retransmitted – the window size is cut dramatically and slow-start redone up to ½ the previous level.
 - (2) From that point on – a slower linear rather than exponential growth is taken.
 - e. These methods when widely implemented allow the Internet to work even in the face of extreme loads.
 - f. Fortunately few people have the ability to re-write their TCP/IP stack and defeat these mechanisms.

C. ARP - Address Resolution Protocol

1. Used as a way for IP to map an Ethernet Address to an IP address
2. When a node wants to send an IP datagram over an Ethernet network, it needs to know the MAC address of the destination.
3. An Ethernet broadcast is sent out asking who owns this IP address
4. The node with the address replies.
5. From the reply the original node gets the MAC address.
6. Now the IP packet can be sent over the Ethernet to the destination.
7. ARP Cache
 - a. The sender keeps a cache of recently resolved addresses so it doesn't have to ARP before sending every packet
 - (1) This cache can often be displayed using “arp” command
 - (2) This cache must time out if one node stops using an IP address and another starts.

- b. When one node sends out an arp reply message, all nodes on a broadcast network may add it to their cache.
8. Proxy-ARP
- a. Sometimes an administrator will want to merge two separate Ethernet networks to look like one for IP packets
 - b. A router can be configured so that it will send an ARP response on an interface for a whole range of IP addresses.
 - c. The router will then receive the packets, and forward them to the correct Ethernet network
 - (1) Will need to do an ARP request on that interface to find the actual node's MAC address.
 - (2) Router will typically be configured to proxy-ARP in both directions.

D. Private IP addresses

1. These are addresses that are not allowed on the Internet so they can be used for private networks.
2. They must either be translated to valid addresses, or kept from accessing the Internet.
3. RFC 1918 Defines:
 - a. 10.0.0.0 - 10.255.255.255 (10.0.0.0/8 prefix)
 - b. 172.16.0.0 - 172.31.255.255 (172.16.0.0/12 prefix)
 - c. 192.168.0.0 - 192.168.255.255 (192.168.0.0/16 prefix)

E. IP – Routing - Chalk talk about system

1. Network 1:
 - a. 10.1.0.0/16
 - b. Node A 10.1.0.10
 - c. Node B 10.1.0.11
 - d. Node D 10.1.0.12
 - e. Node E 10.1.0.13
 - f. Node F 10.1.0.14
2. Network 2
 - a. 10.2.0.0/16
 - b. Node B 10.2.0.11
 - c. Node D 10.2.0.12
 - d. Node C 10.2.0.13
 - e. Node G 10.2.0.14
 - f. Node H 10.2.0.15
3. Network 3
 - a. 10.3.12.0/24
 - b. Node A 10.3.12.10
 - c. Node D 10.3.12.12
 - d. Node C 10.3.12.15
 - e. Node I 10.3.12.13
 - f. Node J 10.3.12.14
4. Discuss route table for Node A, D, H, F
 - a. Assume Node A has:
 - (1) default route of 10.3.12.12
 - (2) 10.1.0.10/16 – Gateway Ethernet 0
 - (3) 10.3.12.10/24 – Gateway Ethernet 1
 - (4) 10.2.0.0/16 - Gateway 10.3.12.15

- b. Assume Node D has:
 - (1) no default route
 - (2) 10.1.0.12/16
 - (3) 10.3.12.12/24
 - (4) 10.2.0.12/16
- c. Assume Node H has:
 - (1) default route of 10.2.0.12
 - (2) 10.2.0.15/16 – Gateway Ethernet 0
- d. Assume Node F has:
 - (1) default route of 10.1.0.11
 - (2) 10.1.0.14/16 – Gateway Ethernet 0
 - (3) 10.3.12.0/24 – Gateway 10.1.0.10

F. DNS - Domain Name System

1. A protocol and the whole system for mapping names of machines to IP addresses
2. The protocol is usually over UDP packets.
 - a. Unreliable, but since message is only one packet to the server and one packet in response it has lower overhead than TCP.
3. A node is typically configured with the IP address of one or more DNS servers.
 - a. If the first one fails to respond, the second one is used, etc.
4. Top Level Domain - the last set of letters after a period (.) in a domain name.
5. Root name server - the master domain name server for a given top level domain.
6. DNS Control
 - a. ICANN - Internet Corporation for Assigned Names and Numbers
 - (1) Created by US government as a way to sort out the management of DNS
 - (2) Very controversial in how it has been handling things
 - b. Each of the top level domains has a single database maintainer
 - (1) .com, .net, .org are all through Network Solutions
 - (2) .gov is controlled by the United States government
 - (3) Each country has a two letter top level domain
 - (a) (.us, .cc, .tv, .ru, .uk, .de, .au, etc.)
 - c. There may be multiple companies that register names into that database, but a single database exists.
 - d. Some people have started creating alternative name servers

III. Presentation Layer

A. ASN.1 & BER

1. ASN.1 - Abstract Syntax Notation One
 - a. A formal language for describing messages that go between computer systems.
2. BER - Basic Encoding Rules
 - a. The method by which messages using ASN.1 are arranged into bits for transmission.
3. Many systems today use ASN.1 with BER to define their message structure.
4. BER typically uses a header for each field that defines what it is, the length, and then the data

B. ASCII - The anti-ASN.1 system

1. Many protocols on the Internet today use ASCII based encoding mechanisms
 - a. HTTP, SMTP, FTP control, etc.

2. ASN.1 encoded messages can not be decoded by just looking at them on a terminal, while ASCII based messages can

C. Network Management

1. SNMP - Simple Network Management
 - a. Uses ASN.1 encoded messages to get/put values in a table type structure
 - b. messages are sent over UDP/IP
 - c. Requests are only simple set's and gets.
 - d. More complex operations can take significant work
 - e. Simplicity allows for very simple (and cheap) devices to implement this protocol. (cheap Ethernet switches for example)
 - f. Everything is a table in SNMP
 - (1) Can be a limitation for more complex devices – requires multiple tables that reference one another
 - (2) Makes life simpler for the devices implementing SNMP
2. CMISE - Common Management Information Service Elements
 - a. Uses an object oriented view of the system
 - b. Many layers of protocols
 - c. A very rich filtering and selection system.
 - d. Promoted and standardized mostly through Bellcore/Telcordia
 - (1) Driven by phone companies desire to have a common management system for everything
 - e. Set of objects is “standardized” but every vendor has their own extensions so the management system must adopt to these extensions.
 - f. Mostly dead system
 - g. So bloated it takes seconds to do a single query
 - h. Requires many megabytes of RAM on managed systems.
3. XML – more details needed here
4. SOAP – ditto
5. CORBA

D. Encryption

1. Encryption is a method by which information is modified so that others can not understand it.
 - a. Scrambling of the data
 - b. aka Cryptography
2. Stenography is a method by which information is hidden from others.
 - a. Hiding of the data using “noise”
 - b. Least significant bits in pictures or audio
3. Encryption has 2 major branches
 - a. Asymmetric Encryption (Public Key)
 - b. Symmetric Encryption
4. Encryption - the players
 - a. Instead of using A sends a message to B, cryptography books have taken to using some relatively standard names for the nodes communicating
 - b. Alice, Bob, Carol, Dave - participants in an communication
 - c. Eve - the eavesdropper - listens in on communication, but doesn't alter the communication.
 - d. Mallory - a malicious active attacker
 - e. Peggy - a prover
 - f. Victor - a verifier

5. Symmetric Key Encryption

- a. Both the sender and the receiver know some common secret.
- b. The secret is the key to decoding the message
- c. The secrecy of the key is important
- d. Transporting and securing the key between the Alice and Bob is difficult, because it must be done through a secure mechanism.
- e. One time pad - the key is as big as the message. The message is xor'd with the key.
 - (1) The only truly unbreakable encryption system.
 - (2) Most products that claim one-time-pad are not.

6. Symmetric Key encryption types

- a. DES - Data Encryption Standard
 - (1) Uses a 56 bit key
 - (2) All 2^{56} keys can be tested in < 24 hours with a \$250k machine
- b. 3DES - Use of DES three times over
 - (1) Gives 3×56 or 168 bits of keyspace
- c. AES - Advanced Encryption Standard
 - (1) Rijndael is the new chosen standard
 - (a) Chosen in October 2000 after 3+ years of competition
 - (b) Officially set as a US government standard in May 2002
 - (2) 128-256 bit key

7. Asymmetric Encryption

- a. Commonly called Public Key encryption
- b. Two numbers (secrets) are created.
- c. One of these keys is called the public key and given to everyone.
- d. One of these keys is called the private key and is kept secret.
- e. To send a message, the public key is used to encrypt the data. After that, only someone with the private key can decode the message.

8. Public Key Encryption types

- a. RSA - Ron Rivest, Adi Shamir, and Leonard Adleman.
 - (1) An algorithm that picks two large prime numbers and multiplies them. It is assumed that it is very very difficult to factor the resulting number.
 - (2) The bigger the numbers the harder it is to break the encryption
- b. Elliptic Curve
- c. Many practical systems use public key encryption to encrypt a symmetric key that is then used to encrypt the rest of the message
 - (1) Public Key encryption tends to use compute expensive algorithms.

9. Key Size

- a. Comparing key size between different algorithms is not easily done.
- b. A typical 128bit symmetric key encryption method might take as long to break as a 1024 bit asymmetric key encryption.
- c. Don't get into "my key is bigger" battles.
- d. What is important is how strong the overall system is.
 - (1) Key size is one factor
 - (2) Algorithm choice is another
 - (3) Use of proven algorithms is best
 - (4) Implementation is often the biggest problem
 - (5) Beware – a lot of people are selling snake oil.

- e. Comparison from “Applied Cryptography” by Bruce Schneier in 1996
 - (1) For similar resistances to brute force attacks –
 - (a) 56 bits Symmetric \approx 384 bits Public-key
 - (b) 64 bits Symmetric \approx 512 bits Public-key
 - (c) 80 bits Symmetric \approx 768 bits Public-key
 - (d) 112 bits Symmetric \approx 1792 bits Public-key
 - (e) 128 bits Symmetric \approx 2304 bits Public-key
 - (2) Security Requirements and the lifetime of information vs. symmetric key length
 - (a) Tactical military information – Minutes/hours – 56-64 bits
 - (b) Product Announcements, mergers – Days/weeks – 64 bits
 - (c) Long term business plans – years – 64 bits
 - (d) Trade secrets (Coca-Cola recipe) – decades – 112 bits
 - (e) Personal affairs - >50 years – 128 bits
 - (f) Diplomatic embarrassments >65 years – 128 bits
 - (g) US census data – 100 years – at least 128 bits

E. Authentication

1. Authentication is the process of making sure that someone is who they say they are.
2. It is also the process of making sure that a message has been transported without being modified.
 - a. Much more than error detection
 - b. Mallory might intercept the message, change it and change the CRC
3. One-way hash
 - a. An algorithm that creates a big hashed number and it is very difficult to produce another message with the same number.
 - b. SHA-1(160 bit hash), MD5 (128 bit hash), RIPEMD (128 bit hash)
4. The secure hash can be sent via another transport mechanism that is secure
5. The secure hash could be encrypted with the sender’s private key – allowing everyone to decrypt and check the secure hash
 - a. This assumes that the sender keeps their private key from being stolen by someone else.

F. Authentication & Encryption

1. Authentication often uses many of the same public key encryption algorithms as encryption.
2. Message tampering detection
 - a. Create a secure hash, and then encrypt using the private key.
 - b. Anyone can then decrypt the hash using a public key and compare the result with their own copy of the public key.