MAXt

please help

* 1. dig MX diktion.net OR nslookup -type=mx diktion.net

telnet smtp.diktion.net 25

* 1. 1. Web server down for maintenance?
     2. DNS request (using UDP) never succeeded and so browser never received a response
     3. website is blocked by the firewall on company’s Access Control List

R =L/(t2 - t1) = (16 \* 10^6 \* 8)/32.

Utilisation = R/(24 \* 10^6) = ⅙.

Utilisation lower because of:

* Slow Start protocol?
* Web server processing other queries alongside PDF, slowing server’s upload rate?
* Line shared with other queries from user?
* You’re at home so maybe someone else is using netflix in the house?
* Utilisation will never be 100% as this requires RTT to = 0
* Diktion’s internet line could simply be less than mine, resulting in a bottleneck on their end

1. Anyone using software (e.g. Wireshark) could sniff packets on network (using Monitor Mode) through using the Wireless Access Point.
2. SMTP requests are plaintext => would be able to read contents wee of packets sent to mail server?
3. MITM attack. You could have just connected to someone else’s device and they can see all the traffic.
4. Could have connected to an “Evil Twin”. An access point with the same SSID as the legitimate access point.
   1. TCP.

* Reliable
* Error correction
* Not live-streamed so speed is not that important. Also because the videos already exist, they can be served by CDNs which makes streaming pretty fast anyway.
* Content is buffered so there should be some way if the connection slows down before the user starts noticing it
* service is paid: need to ensure Quality of Service for users
  1. g = 9, p = 11, a = 2, b = 5

Public values: y = g^a mod p = 81 mod 11 = 4

x = g^b mod p = 59049 mod 11 = 1

Shared key = y^b mod p = x^a mod p = 1\’iuy

e(HELLO, 1) -> IFMMP

1. 1. 1. BGP - Inter AS gateway protocol. Manages how packets are routed through the internet by exchanging routing information between ASs. Layer 4 (Transport layer)

(BGP does what is considered a layer 3 role and most routing protocols are layer 3 but BGP is layer 4 because it used TCP / There is no god)

* + 1. Think it’s this. Layer 1? <https://en.wikipedia.org/wiki/Shannon%E2%80%93Hartley_theorem>
    2. Concept of a token passed between devices, where devices can only transmit frames while holding the token. Data Link layer.
    3. A device that repeats packets to devices with a MAC address corresponding to MAC address of destination. Ethernet is a Data Link layer protocol and use of MAC addresses => Data Link layer.
  1. Is this a joke. I hope so. But it means we won’t get it hopefully :) - Can we safely assume this will never happen again? :DD
     1. A: Total length

B: Time To Live

C: Source Address

D: Destination Address

* + - 1. Version indicates whether IPv4 or IPv6.
      2. Hlen - header length in 32 bit words
      3. Type of service - Can be used to specify a priority
      4. Identifier - Used to identify IP packets from the same upstream packet
      5. Flags - Reserved bit / Don’t fragment bit / More fragments bit
      6. Fragmentation offset is offset (in units of 8 bytes) that indicates how far into the original data the packet starts at.x
      7. Header checksum is used to check whether data is corrupted (after transmission, it is recalculated data and compared; if mismatch needs to retransmit). [Redundant becau from se of Ethernet checksum?]
      8. Options - optional fields in IP packet.
      9. Protocol - Such as ICMP, TCP, UDP, etc
    1. 1. Hlen - No longer need ed as the header is of fixed size (40 bytes)
       2. Flags - IPv6 packets are not fragmented by routers. When fragmentation is done by hosts, extension headers can be used.
       3. Type of service - Replaced by traffic class field
       4. Identifier not required as packets can be identified by their TCP headers ur mum
       5. Header checksum - Headers are rarely corrupted nowadays. Even if they are they will be handled by higher protocols.
       6. Protocol - Replaced by next header field
       7. Fragmentation offset removed as for IPv6 fragmentation only occurs at end systems.
       8. Options – usually not used anyway; need space for address fields + provides fixed size header
    2. -Source and destination address fields are only 6 bytes each in an ethernet frame. IPv6 addresses are 16 bytes.

-Max data length is only 1500 bytes in an ethernet frame. Increases fragmentation

-Lack of flexible options in Ethernet header, difficult to add new features/update how packets are handled unlike IPv6 with the presence of next header field and extension header

-No hop limit to prevent packets looping around infinitely

-MAC address, cant use that mate