The golden age of hacking

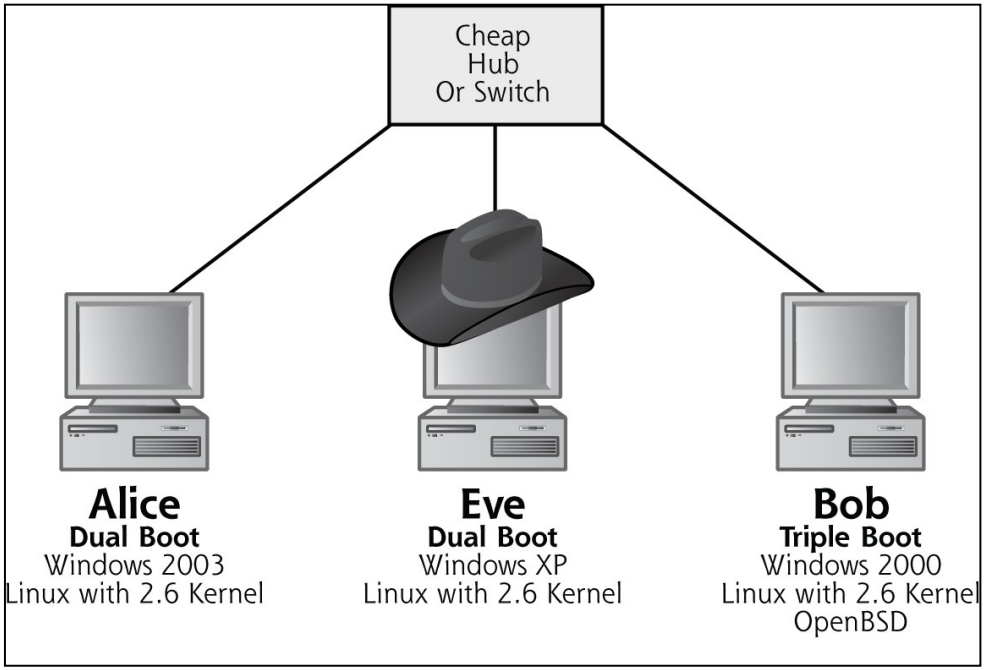
Pen-test intro

TCP/IP

Networking overview

Naming names

- Usually attacker(s)/bad guy(s) are used instead of
  - Hackers, crackers, black hats etc.
- Remember that the tools could hurt you bad!
  - Using the tools – incidentally or by purpouse
  - Web sites
  - Searching
- Lab for experiments
  - Alice
  - Bob
  - Eve



Common phases of the attack - SANS

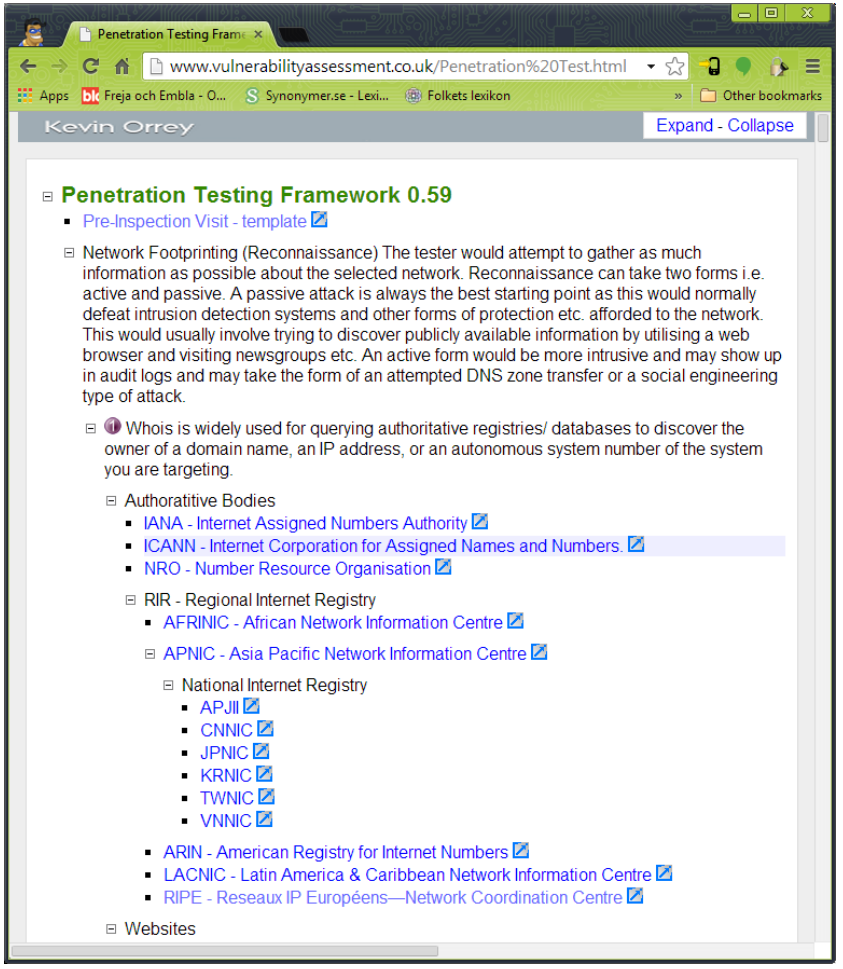
- **Foot Printing/Reconnaissance**
  - This is the step where we want to get as much information about our opponent without being intrusive. Things like target address ranges, namespace acquisitions, and information that will be beneficial in deeper attacks.
- **Scanning**
  - This is where we want to assess our opponent's systems. What operating system do they use? What ports are they listening on? We are looking for vulnerable places to enter into their systems.
- **Enumeration**
  - Next, we go a little deeper in our attacks to attempt to identify valid user accounts or poorly protected network shares.
- **Gaining Access**
  - Now that we have some information, we begin to attempt to access our opponent's computers.
- **Escalating Privilege**
  - If we have gained a low-level user account, we will now escalate our privilege to that of an administrator equivalency.
- **Creating Backdoors/Maintaining Access**
  - We do not want to loose our access to our opponent's machines; hence, we create backdoors to come back in with privileged access.
- **Covering Your Tracks**
  - Not getting caught, or not having our "new" accounts be erased is important, so we need to hide our activities.

Common phases of the attack - CHR

- 1. Reconnaissance
  - Google searches and DNS interrogation etc.
- 2. Scanning
  - Enumeration, war driving
- 3. Gaining access at the operating system and application level
  - Buffer overflows, password and web application attacks etc.
- 3. Gaining access at the network level
  - Sniffing, session hijacking
- 3. Denial-of-service attacks
- 4. Maintaining access
  - Backdoors, trojans, rootkits
- 5. Covering tracks
  - Logs, covert channels

PTF (Pen Test Framework)

- Pen Test Framework, Compliance tests, Pre-site inspection, Report template etc.
  - http://www.vulnerabilityassessment.co.uk/



Penetration testing – What? Why? How?

- Penetration testing – What?
  - Tries to access computers/documents (information)
  - Tries to bypass security components
  - Tries to elevate privileges
- Penetration testing – Why?
  - Knowledge of how the enemy operates is necessary to build adequate protection
  - If users/administrators know that their systems will be attacked they tend to care more about security
- Penetration testing – How?
  - Anyway we can
    - Almost
  - Tools and information is available on the Internet “By hackers for hackers”
  - The tools must be verified in a controlled environment

Penetration testing – Tools?

- Security/vulnerability scanners
  - General: Nessus, Rapid7 NeXpose, (more exists)
  - Application specific: Nikto2, w3af, (many more exists)
- Updated modules for new vulnerabilities
- Automation – all machines are treated equally
- Reports are generated by the tools
- Security/vulnerability scanners - disadvantages
  - False positives
  - Reports are often hard to understand
  - Limited capabilities
    - No sniffing
    - No spoofing

http://en.wikipedia.org/wiki/Vulnerability_scanner

Vulnerability Assessment vs. Penetration Test

Vulnerability Assessment

Customer Maturity Level: Low to Medium. Usually requested by customers who already know they have issues, and need help getting started.

Goal: Attain a prioritized list of vulnerabilities in the environment so that remediation can occur.

Focus: Breadth over depth.

Penetration Test

Customer Maturity Level: High. The client believes their defenses to be strong, and wants to test that assertion.

Goal: Determine whether a mature security posture can withstand an intrusion attempt from an advanced attacker with a specific goal.

Focus: Depth over breadth.

- http://danielmiessler.com/writing/va_vs_pt/

Penetration testing – How?

- Find and exploit vulnerabilities
- Simulate attacks that are
  - Initiated from the inside - customer depending
  - Expensive, if something goes wrong
  - Expensive to restore
  - Social consequences
- Generate a report, describing
  - Actions taken
  - Possible countermeasures
- Focus on IT-systems
- Analysis to gain further access
- NOT to extract actionable intelligence

Penetration testing

- Important to remember!
- If successful
  - **ONE** scenario is proved to be successful
- If not successful
  - IT-security is a moving target
  - Systems evolve (new versions and patches)
  - New vulnerabilities are discovered in old systems
- Attacking a system
  - Easy
  - Find a flaw (can be hard, sometimes)
  - Exploit it
  - Done!

Protecting a system

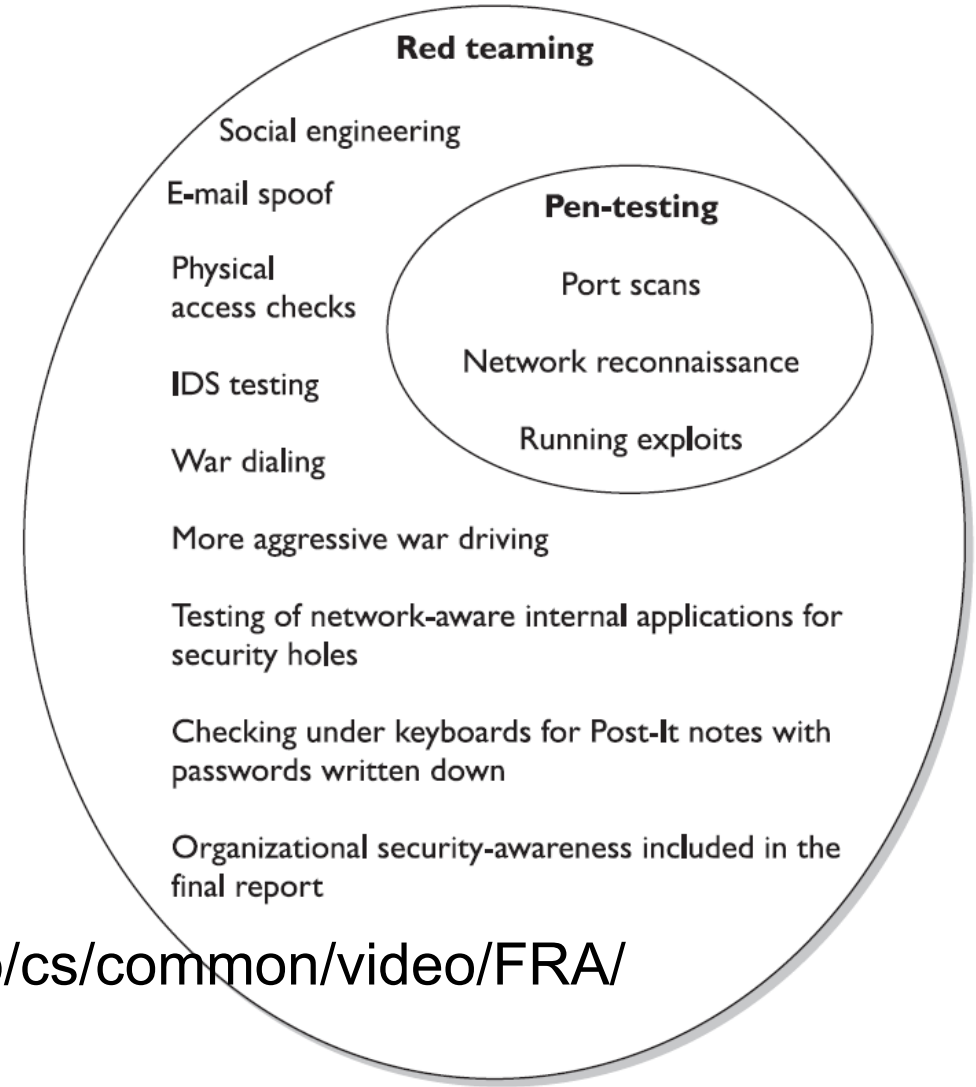
- Hard, very hard
- Find a flaw (as hard as when attacking)
- Correct the flaw (easier than exploiting it)
- Find the next flaw and correct it
- Repeat until there are no flaws left
- Correct the flaw that were left even though you didn’t find them
- Start over from the beginning because now you got a new OS ☺

Penetration testing – Why bother?

- Mainly two reasons
  - Temperature reading
    - How bad is it?
    - Motivation boost
    - Fundraiser for security investments
  - Proofreading
    - What did we forget?
    - Will our system stand an attack from a skilled adversary?

Difference between pen-testing and red teaming

- While pen-testing is great at showing how deeply an attacker can get into a network, **red teaming** should show **all the ways** an attacker can get in
- Movies
  - http://users.du.se/~hjo/cs/common/video/FRA/



Contracts, safety and staying out of jail

- Do not start out with a simple, ad hoc contract for your engagements!
- Working on a customer's production network is a risky business
- Before any work is done for any customer, a few things must be in place
  - First, the customer must completely understand the types of tests your team will be conducting
  - Your team chief must explain the good, bad and the ugly of what could take place during the tests
  - The next thing that must be in place is a solid contract (with the right person) and a document that outlines the scope of the assessment, including the specific tasks that will take place
- There are documented cases where security professionals cracked customer's passwords without the customer's knowledge and without password cracking being listed as part of the contract
- Teams have been fired and security professionals have even got arrested!

OSI-modellens 7 olika nivåer

- OSI-modellen är en referensmodell för datakommunikation
  - http://sv.wikipedia.org/wiki/OSI-modellen
- Den har skapats för att visa hur olika system kan kommunicera med varandra

7. Applikationsnivå: Koppling till användaren, hur programmet skall visa den överförda informationen.

6. Presentationsnivå: Beskriver vilka koder som används i överföringen av data, behandling av komprimering och kryptering.

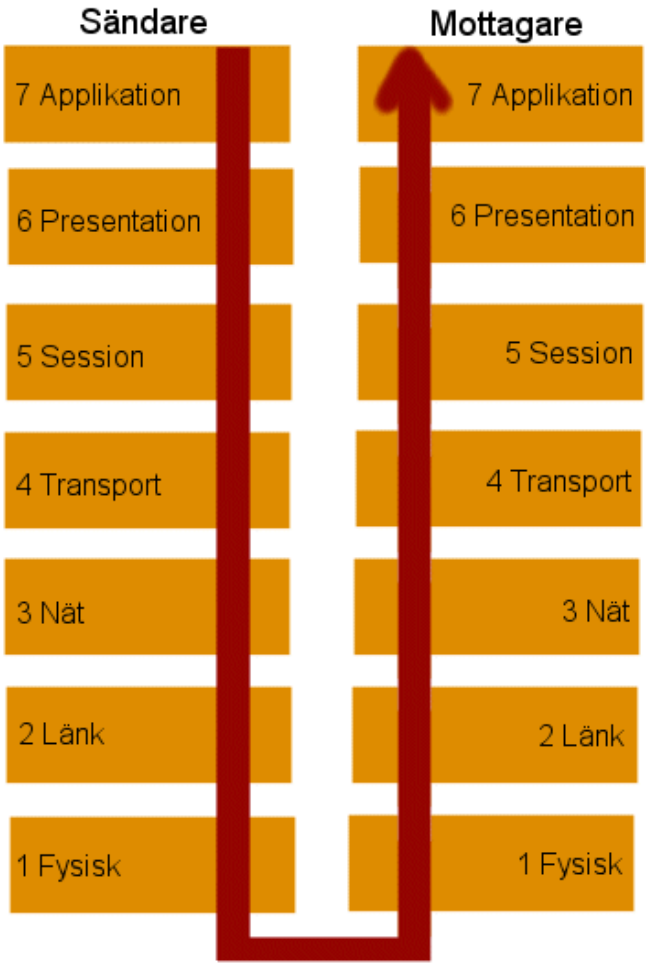
5. Sessionsnivå: Bestäms hur den logiska uppkopplingen och dialogen ska genomföras mellan sändare och mottagare, dvs. applikations protokollet, t.ex. HTTP.

4. Transportnivå: Här bestäms vilket bärarprotokoll som ska användas vid överföring av data från sändaren till mottagaren, t.ex. TCP.

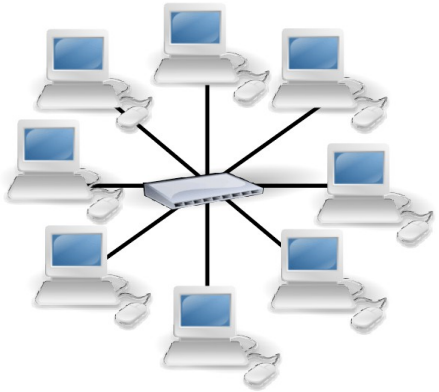
3. Nätnivå: Adressering, vägval, anpassning till protokollet som används i det fysiska nätverket. T.ex. IP

2. Länknivå: Kontrollerar att överföringen i kommunikationskanalen fungerar korrekt.

1. Fysisk nivå: Beskriver vilket gränssnitt som används.



Topologier och media i nätverk



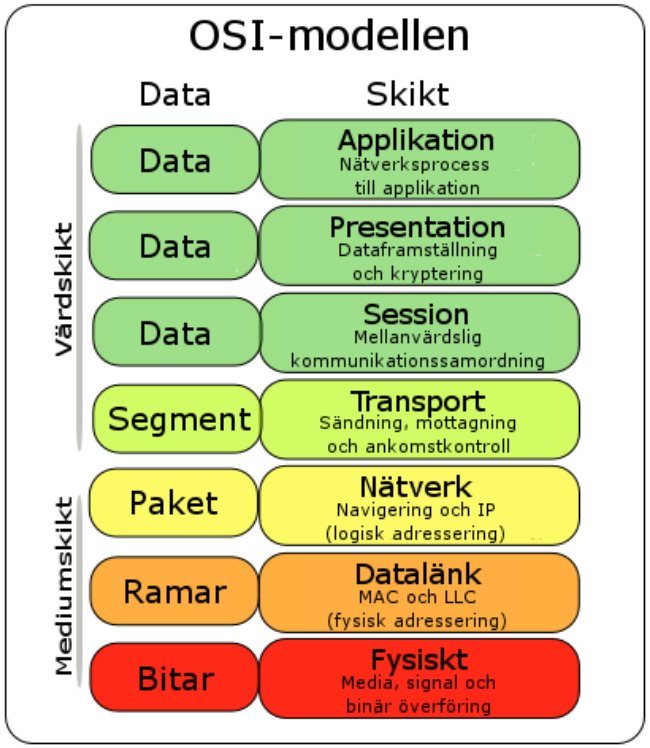
Stjärnformat datanät

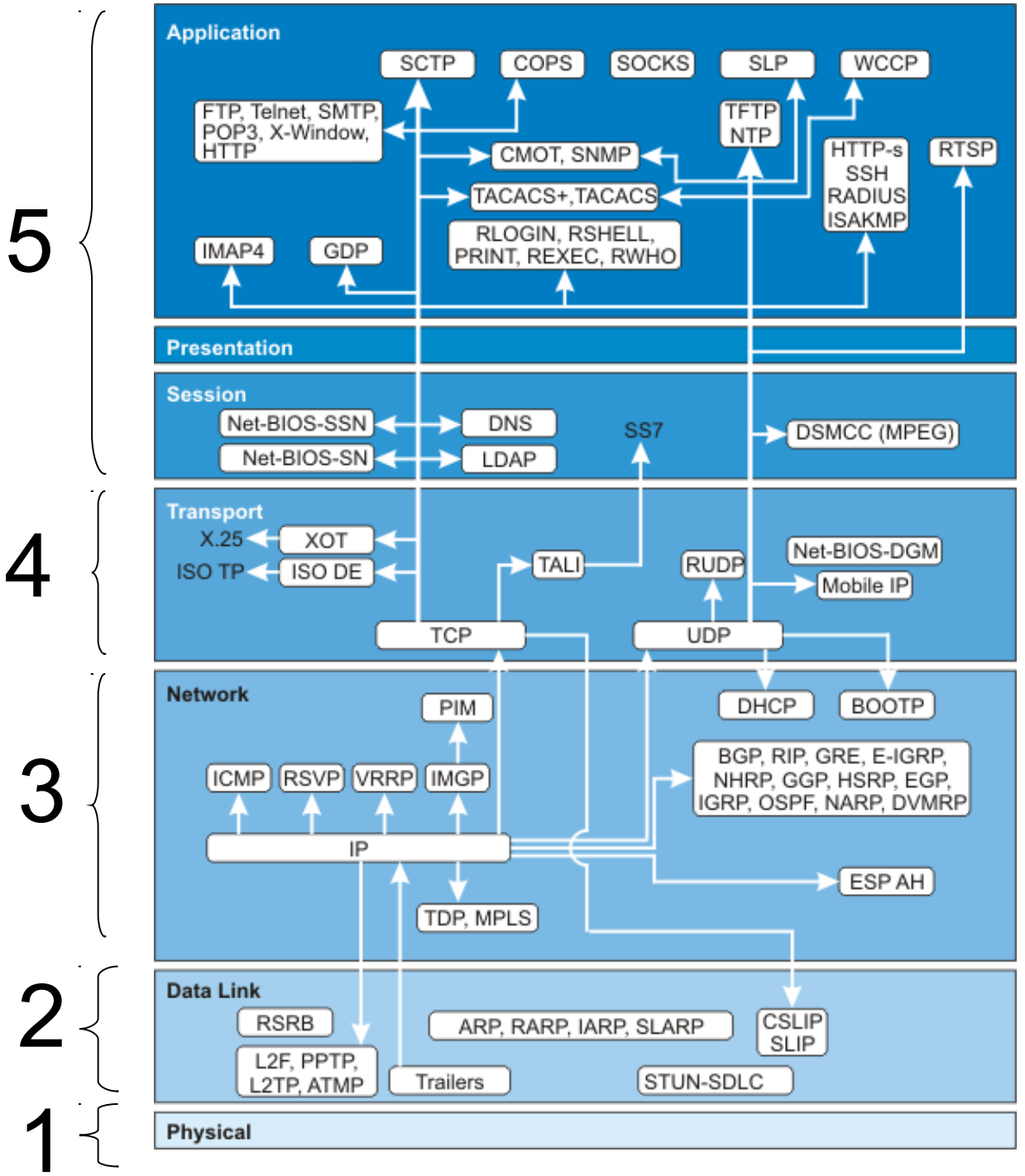
- Fysiskt
  - Koaxialkabel
  - Partvinnad kopparkabel
  - Fiberoptisk kabel
- Länk
  - Trådlös bärarvåg
    - WLAN, WWLAN as WCDMA (HSPA/HSDPA/HSUPA/HSPA+), LTE etc.
  - CSMA/CD (C*arrier Sense Multiple Access with Collision Detection*) eller ethernet (används till 99,9% i LAN)
    - Broadcast, unicast, multicast
  - Token ring (utdött), PPP, ATM etc.
- Trusted (work or home) och untrusted (public) nätverk
  - Avlyssning
  - Skalskydd
    - Firewall, Proxy, NAT

Transmission Control Protocol/Internet Protocol (TCP/IP)

- Utgår från DARPA-modellen med 4 lager
  - http://en.wikipedia.org/wiki/TCP/IP_model
  - 5. Applikationslagret
    - Motsvarar i stort sett de 3 översta lagren i OSI-modellen
  - 4. Host till host transportlager
    - Motsvarar i stort sett transportlagret i OSI-modellen
  - 3. Internetlagret
    - Motsvarar i stort sett nätverkslagret i OSI-modellen
  - 2. Nätverkskontaktlager
    - Motsvarar lager 2 (länklagret) i OSI-modellen
  - 1. Fysiska lagret
    - Motsvarar lager 1 i OSI-modellen

The five-layer TCP/IP model



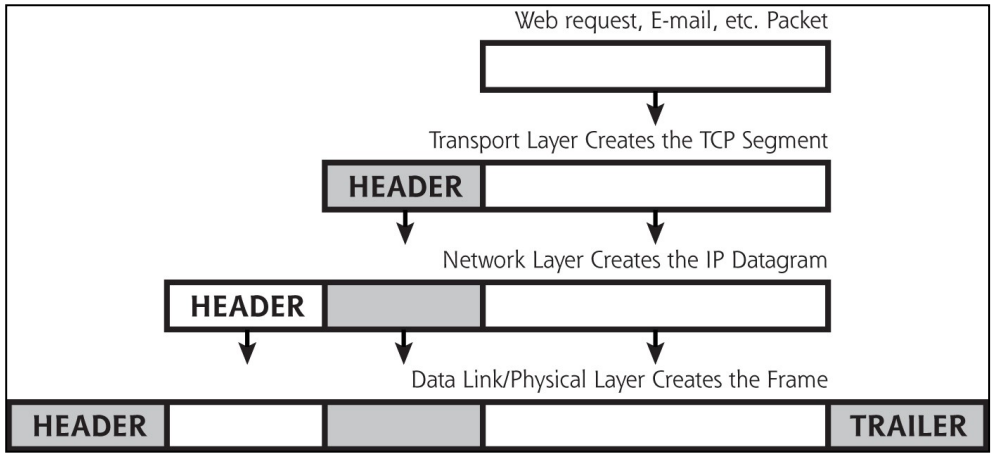


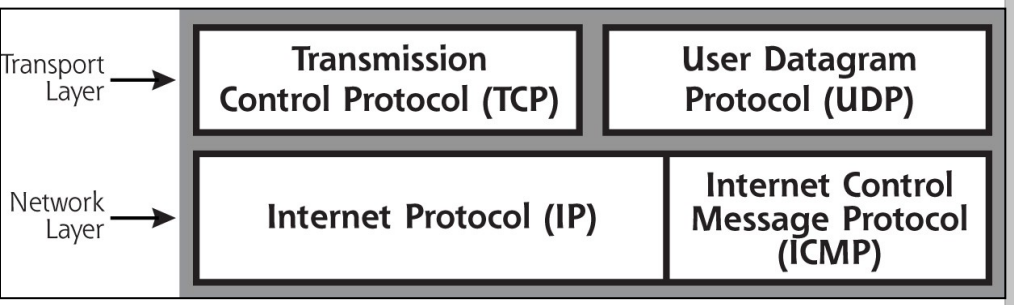
Några vanliga TCP/IP protokoll

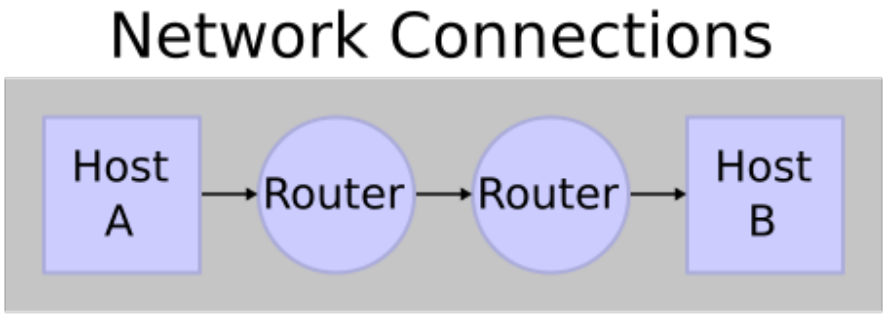
- IP (Internet Protocol)
  - Adresserar och routar paket mellan värddatorer (hostar)
- ARP (Adress Resolution Protocol)
  - Översätter hårdvaruadresser (MAC – Media Access Control) till IP-adresser
- ICMP (Internet Control Message Protocol)
  - Kontrollerar att paketleverans fungerar
- IGMP (Internet Group Management Protocol)
  - Hanterar hostar som är med i multicast grupp, kräver stöd från router, motsatsen till unicast
- TCP (Transmisson Control Protocol)
  - Pålitligt förbindelseorienterat, sekvens nummer skickas, använder portar
- UDP (User Datagram Protocol)
  - Opålitligt förbindelselöst, använder portar, snabbare än TCP

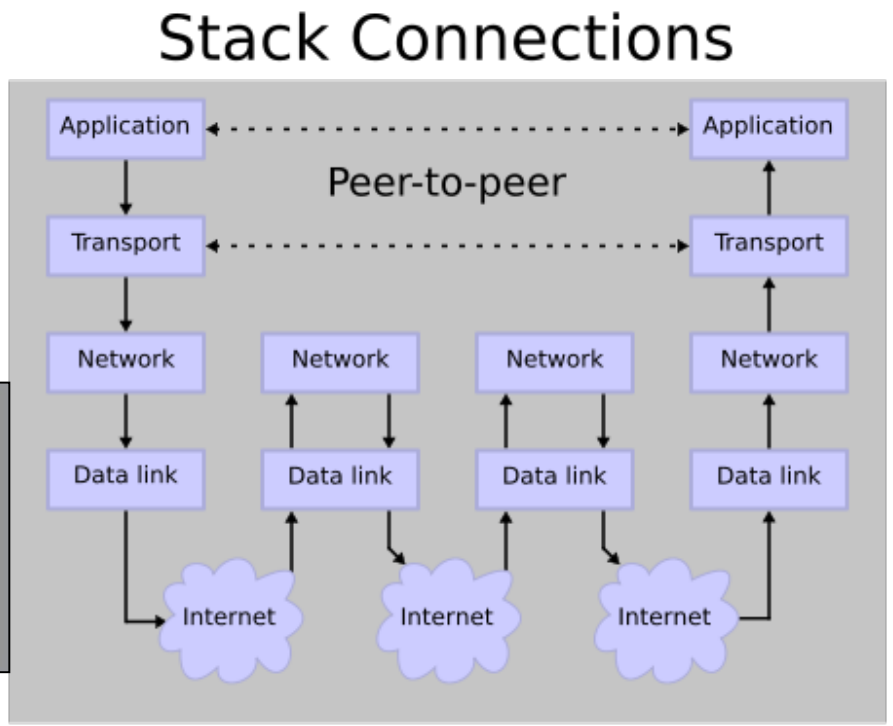
Networking TCP/IP

- Basic knowledge is implied from experience or earlier courses!





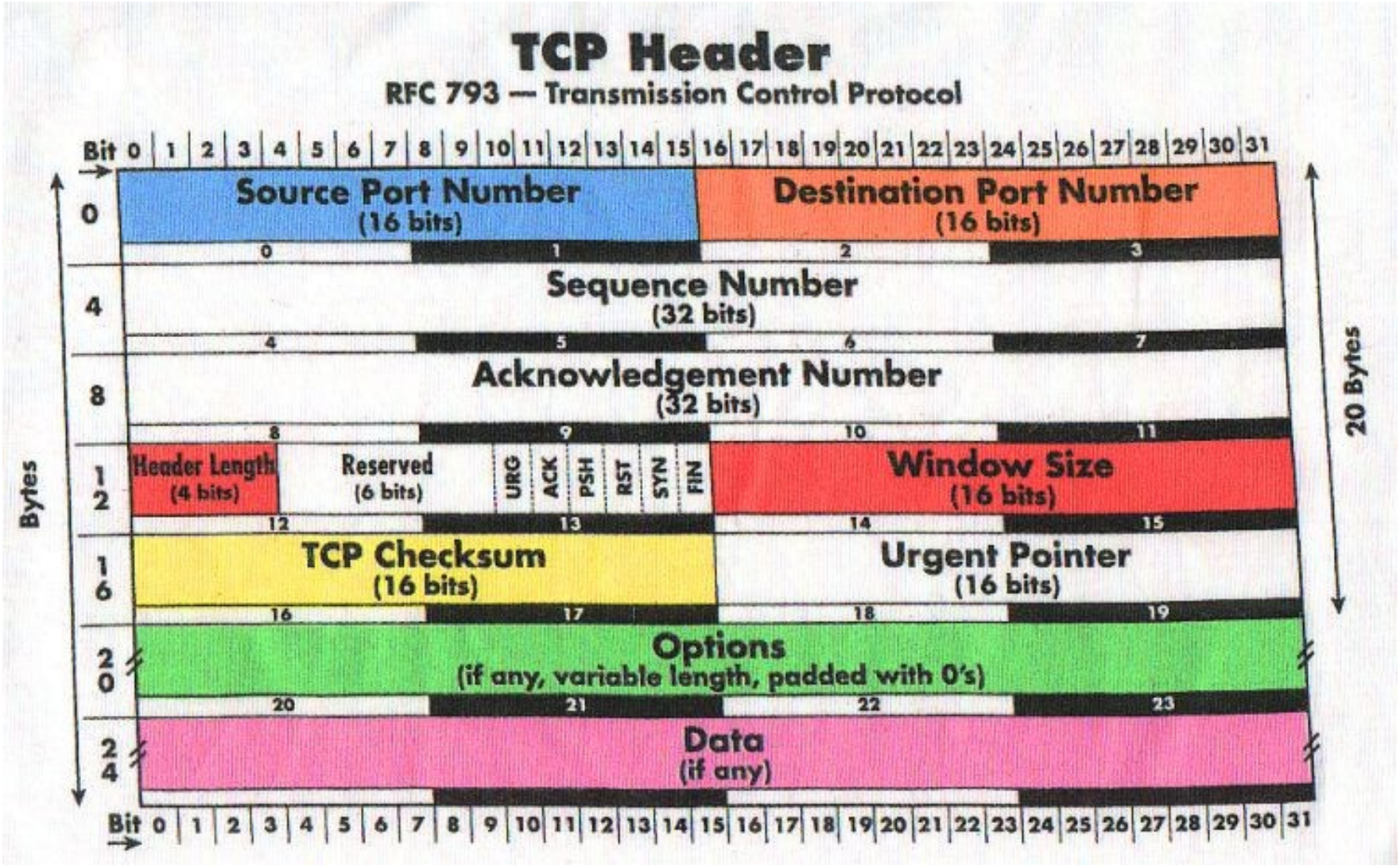




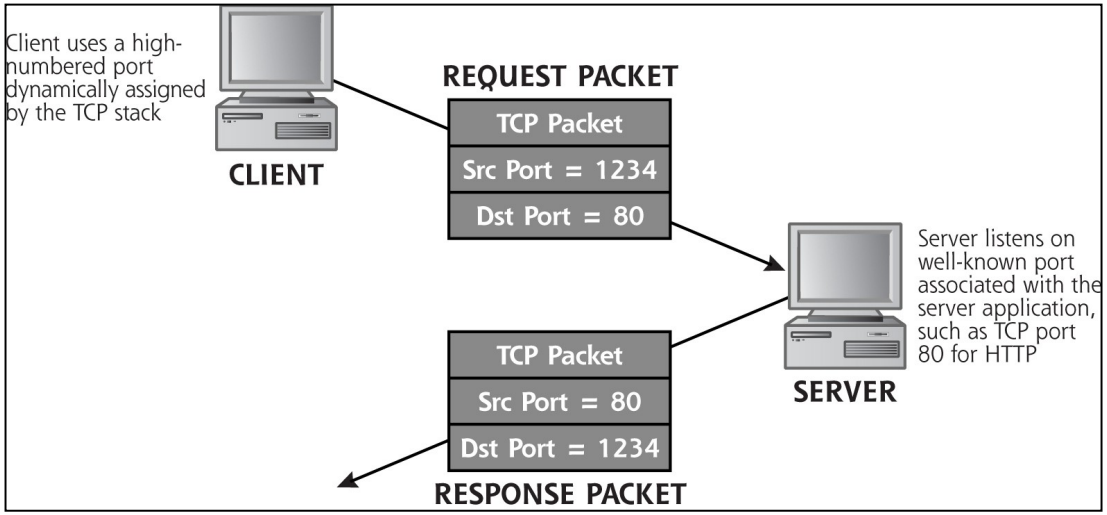
Nätverkstjänster

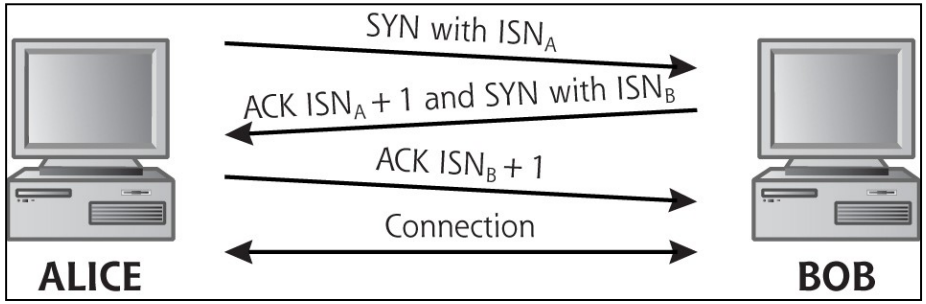
- För att fungera i nätverk måste OS ha vissa nätverkstjänster igång
  - Man bör sträva efter att **endast** ha de **nödvändiga** igång
- Standardtjänster har vissa ”portnummer” tilldelade
  - Portar, kan jämföras med TV eller radiokanaler, 65536 st.
  - Med kommandot netstat kan man se vilka portar som är aktiva
  - Vissa protokoll/applikationer kräver en viss port tex. HTTP (WWW) = 80, FTP (File Transfer Protocol)= 21, SMTP = 25, DNS = 53 (Domain Name System) samma funktion som vita sidorna i telefonkatalogen, se fullständig lista: http://www.iana.org/assignments/port-numbers
  - Well-known ports < 1024 vs. registered ports 1024 – 49151 vs. dynamic/private ports 49152 - 65535

TCP paketstruktur
Header and data 1



TCP paketstruktur Header and data 2

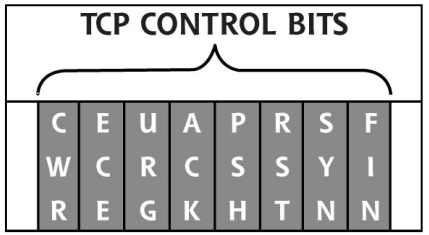




- Source port
- Destination port
- Sequence number
  - Om SYN flaggan är satt så är detta ISN (Initiala Seq.Nr) och den första databyten är ISN+1, annars är det Seq.Nr för första data byten i förbindelsen
- Acknowledgement number
  - Om ACK flaggan är satt är detta nästa Seq.Nr som sändaren förväntar sig att motta. Normalt alltid satt efter synkroniseringen.
- Header length (Data offset)
  - Specify where header ends and data starts. Equal to TCP-header size in 32-bit words, min 5 and max 20 => 20 – 60 bytes
- Reserved (6 bits) – för framtida användning

TCP paketstruktur - Header and data 3

- Flags (kontroll bitar)
  - URG – Urgent pointer är satt, data needs to be handled quickly
  - ACK – Ack är satt, verifierar att tidigare paket är korrekt
  - PSH – Push funktion, flush data thru TCP layer don't wait
  - RST – Resetta förbindelsen
  - SYN – Synkronisera sequence nummer, tex. vid sessionens start
  - FIN – Ingen mer data från sändaren
- Nya flaggor (RFC 3168)
  - CWR – Congestion Window Reduced
  - ECE – Explicit Congestion Notification Echo



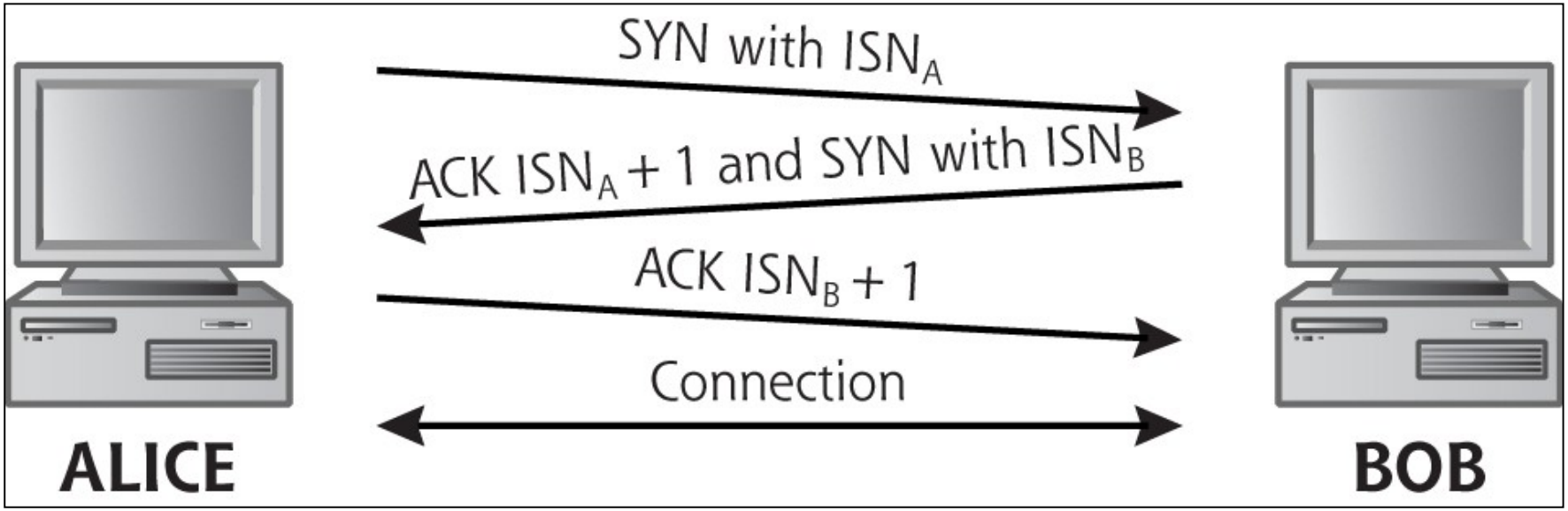
- Window size – antalet bytes (octets) sändaren av detta segment är villig att ta emot
- TCP Checksum – 16 bitars kontrollsumma på header och data
- Urgent pointer – om URG är satt så är detta en positiv offset till slutet för urgent data
- Options – ytterligare options som t.ex. TCP max size etc. och padding
- Data – tillhör ej header, varje sänd databyte räknar upp Seq.Nr

Mer om TCP/IP

- En TCP socket (anslutningsport) har följande tillstånd
  - LISTEN, väntar på anslutning från remote host (TCP port)
  - SYN-SENT, väntar på att remote TCP host ska sända paket med SYN & ACK
  - SYN-RECEIVED, väntar på att remote TCP host ska sända tillbaka ACK efter att lokal TCP host sänt connection ACK
  - TIME-WAIT, väntar tillräckligt länge på att remote TCP ska ha fått ACK på dess connection termination request
  - Övriga tillstånd
    - ESTABLISHED, FIN-WAIT-1, FIN-WAIT-2, CLOSE-WAIT, CLOSING, LAST-ACK, CLOSED
- TCP har 3 tillstånd (se följande slides)
  - Anslutning etablering
  - Data sändning
  - Anslutning terminering

TCP/IP - Anslutning etablering

- TCP anslutning använder 3-vägs handskakning
  - Passive Open
    - Innan en Alice försöker ansluta till Bob så måste Bob binda en port för att kunna öppna den för anslutningar
    - När passive open är klart för bob kan Alice initiera active open
  - Active Open
    1. Active Open görs genom att Alice sänder SYN till Bob och ISN A (Init SekvensNummer)
    2. Bob svarar med ACK på ISN A+1 och SYN med ISN B
    3. Alice sänder slutligen ACK till Bob och ISN B+1
- Iom. detta har både klient och server mottagit ACK för anslutningen

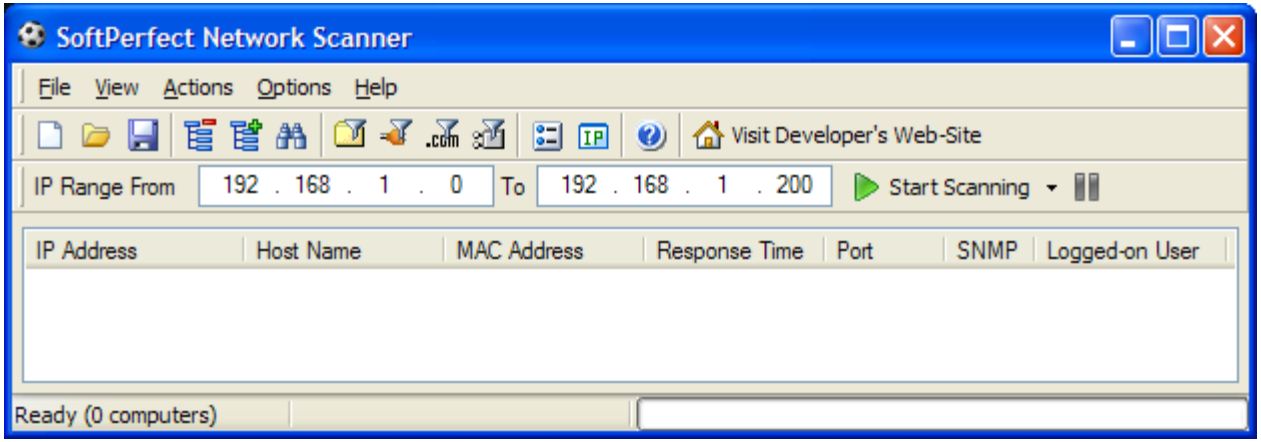


TCP/IP – Data sändning

- Nyckelfunktioner
  - Felfri datasändning som är ”i ordning”
  - Omsändning av ”tappade” paket och uteslutning av duplicerade paket
  - ”Congestion throttling” – flödes kontroll
  - I de 2 första stegen i 3 vägs handskakningen så utväxlas ett ISN (Initial Sequence Number) som identifierar ordningen mm. på sändningarna, räknas upp för varje sänd data byte i förbindelsen
- Window size (TCP headern)
  - Mängden mottagen data som kan buffras upp innan ACK sänds från mottagande värd
- Window scaling
  - Öka/minska storleken av window size i nätverk med hög/låg bandbredd

TCP/IP – Anslutning terminering

- TCP terminering använder 4-vägs handskakning
  - Oberoende terminering av varandra
  - När någon värdarna vill avsluta sessionen sänder den ett FIN-paket som besvaras med ACK, dvs. 2 FIN och 2 ACK behövs
  - En connection kan vara ”half-open”, dvs. en sida har terminerat
- En half-open anslutning brukar tima ut efter omkring 3 minuter
- Med en nätverksskanner eller portskanner kan man från en annan dator se vilka portar ”victim” svarar på för att hitta startade tjänster, t.ex. SuperScan, NMAP etc.
  - Verifiera att det verkligen är din tjänst som svarar och inte något slags malware! Använd **”banner grabbing”**
  - En personlig eller central brandvägg kan kontrollera vilka TCP/UDP portar som tillåts fungera på datorn respektive in/ut i nätverket



SYN floods

- Attacken går ut på att klienten använder en IP-adress som inte svarar servern – vilket skapar en halvöppen anslutning
- Varje halvöppen anslutning konsumerar resurser hos servern och till slut kan de vara helt förbrukade
  - Endera för applikationen eller hela servern
- Det är svårt att skydda sig mot SYN flood attacker
  - Vissa OS kan dynamiskt sänka time-out tiden under tung belastning
- Vissa routrar och brandväggar har delvis inbyggt skydd
  - Intercept mode
    - En mjukvara svarar klienten (i stället för servern) och om klienten sänder ACK så kopplar den transparent upp klienten och servern på riktigt
  - Watch mode
    - En mjukvara övervakar förbindelsen, om allt går rätt till så gör den inget, om inte så sänder den RST (reset) till servern

Sammanfattning TCP/IP

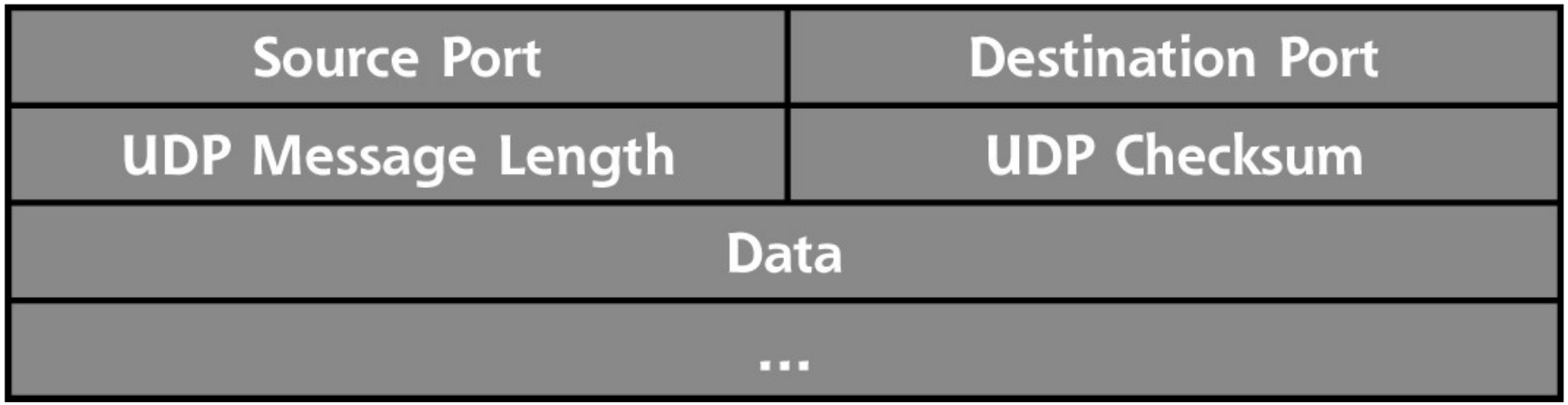
- Pålitlig leverans av data i ordning över ett nätverk mellan två anslutna värdar
- Applikationer sänder byte-strömmar av data och TCP hackar sönder dessa till lämpliga segment, MTU (Maximum Transmission Unit)
- IP levererar paketet till det andra värdsystemet, där det packas upp
- TCP ser till så att inget paket förloras genom att ge det ett sekvensnummer (första byten i data)
- Ett ACK sänds tillbaka om sändningen lyckades
- CRC (checksumma) används, sänds med och beräknas
- Om sändningen misslyckades eller om RTT (Round-Trip Time) överskridits så sänds paketet om
  - The RTT time is calculated from the 3-way handshake by measuring the time between segment transmission and ACK receipt

Mer om TCP

- TCP över Wireless
  - Ej optimerat för denna typ av nätverk
- Debugga/analysera nätet med paketsniffer
  - Promiskuöst mode tar bort adress-filtrering (ser all trafik)
  - Tcpdump och Windump, Wireshark, ettercap mfl.
  - Winpcap library lista: http://www.winpcap.org/misc/links.htm#tools
- Svagheter och alternativ
  - Omsändningsgaranti
    - Programvaror kan inte få tillgång till data om ett paket tappats bort förrän det felaktiga paket omsänts
  - Ganska komplext
    - En hel del buggar har existerat och existerar ännu?
  - Ej lämpligt i system med hög bandbredd
    - Där TCP är olämpligt kan UDP användas (stateless)
  - SCTP (Stream Control Transmission Protocol) – kombinerar TCP och UDP med nya funktioner
    - http://en.wikipedia.org/wiki/Stream_Control_Transmission_Protocol

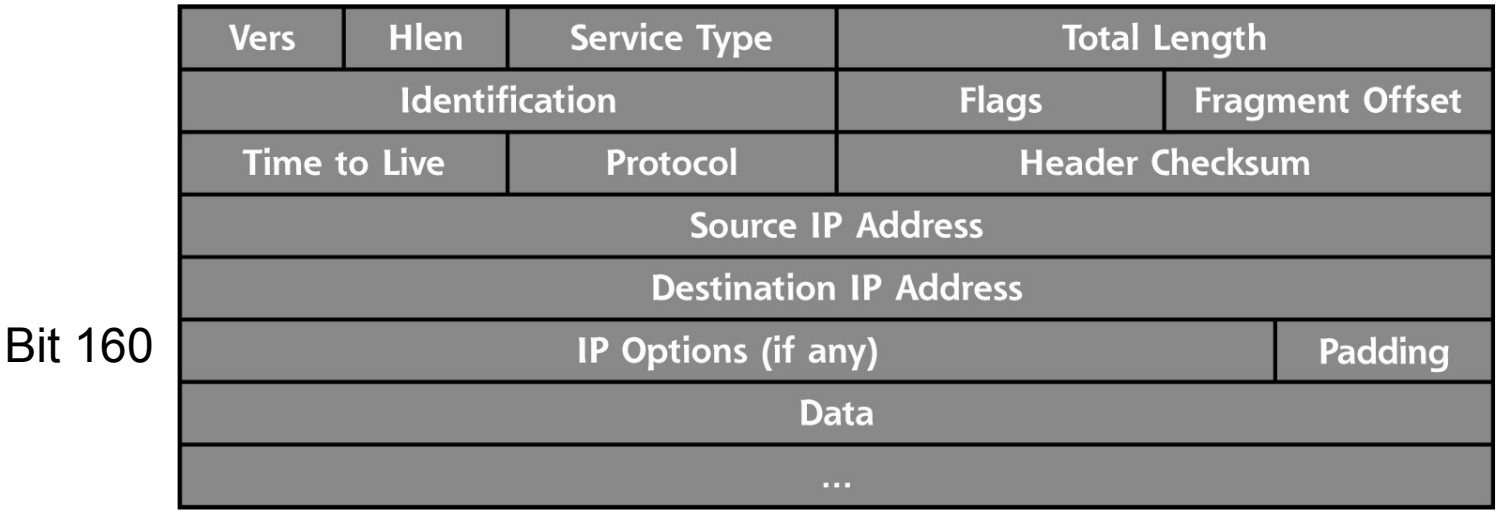
User Datagram Protocol (UDP)

- Used mostly in streaming and query/database applications as DNS, SNMP and TFTP
- Connectionless!
  - Does not know any state, no SYN, ACK etc. as in TCP
- Tradeoff is speed!
- Hard for firewalls etc. to inspect – insecure
- http://en.wikipedia.org/wiki/User_Datagram_Protocol



Internet Protocol (IP) and Internet Control Message Protocol (ICMP)

- IPv4 vs. Ipv6 (different header) - have ICMPv4 and ICMPv6
- IP header is added to front of TCP/UDP/ICMP packet

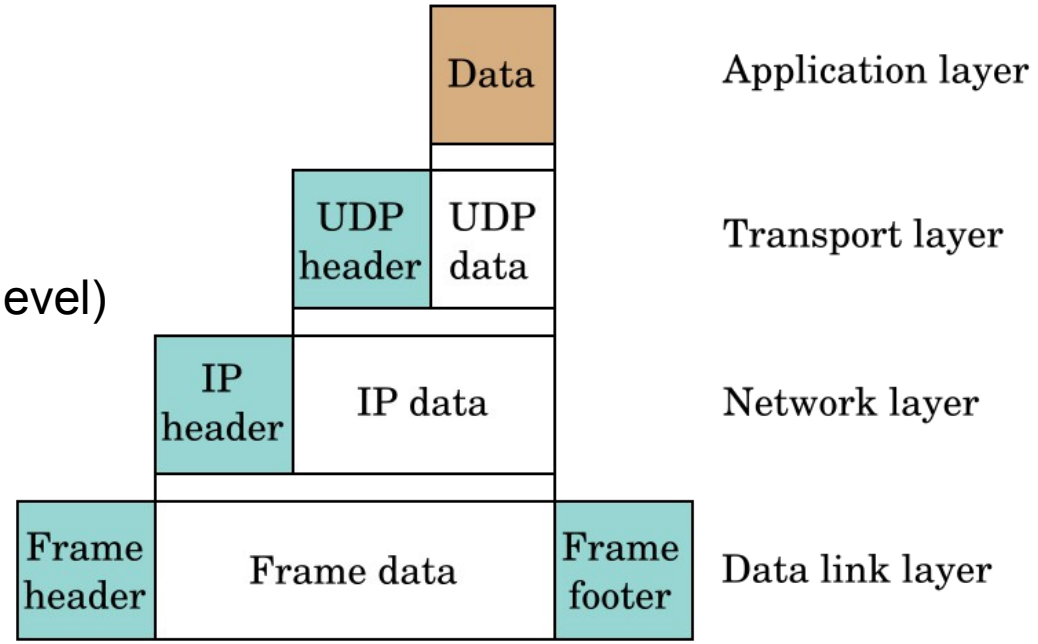


- ICMP transmit command and control information
- ICMP uses the same header format as IP
- Ping and traceroute uses ICMP
- Note, ICMP (and IP) does not use any port number

http://en.wikipedia.org/wiki/IPv4

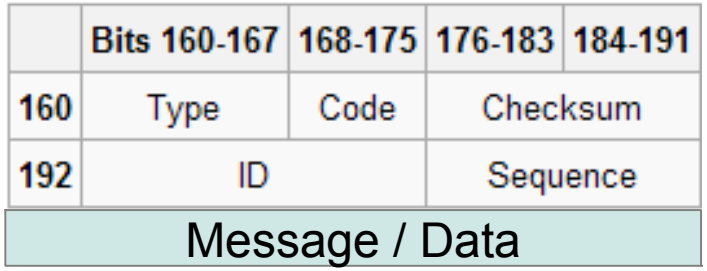
IP v4 Header (page 50 CHR)

- IP packet fragmentation (fragment id, bits and fragment offset in header)
  - Technique used by attacker for stealthy scans, avoid IDS etc.
- Version – 4 bits
- Hlen – Internet header length, total header length
- Service type – Quality of service
- Total length
- Identification – fragment id
- Flags – fragment bits
- Fragment offset
- Time-to-Live
- Protocol – in data (for next level)
- Header Checksum
- Source IP address
- Destination IP address
- Options
- Padding

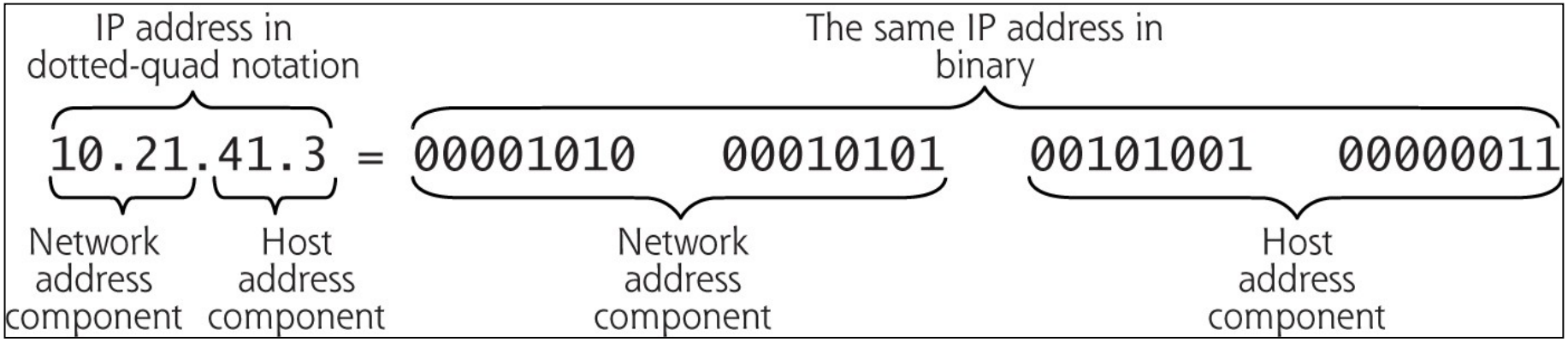


Some ICMP v4 message types (added in IP data)

- The ICMP header starts after bit 160 of the IP header (unless **IP options** are used)
- Type
  - Some ICMP control messages specified below
  - Echo Reply/Request, Destination Unreachable, Time Exceeded etc.
  - http://en.wikipedia.org/wiki/Internet_Control_Message_Protocol
  - http://www.art0.org/networking/the-icmp-protocol-explained
- Code
  - Further specification of the ICMP type; e.g. : an ICMP Destination Unreachable (type=3) might have this field set to 0 through 15, each bearing a different meaning
- Checksum
  - This field contains error checking data calculated from the ICMP header+data, with value 0 for this field
- Rest of header will vary depending on Type and Code. Example: T=0, C=0
  - ID
    - This field contains an ID value, should be returned in case of ECHO REPLY.
  - Sequence
    - This field contains a sequence value, should be returned in case of ECHO REPLY



IP addresses and Netmasks



- Classless Inter-Domain Routing (CIDR)
  - 10.21.0.0/16 – eg. 16 ’1’ bits in the netmask (1 class B net)
  - Subnet Calculator
    - http://www.warriorsofthe.net/utils/index.html