Övningar – Nätverksteknik IPv4 Del2

Ett par instuderingsuppgifter som handlar om Nätverksteknik IPv4 (Del 2).

1. Till vad används *Default Gateway* IP-adressen?

2. Beskriv hur kommunikation går till när en dator ska skicka ett IP-paket till en annan host på det lokala nätverket. (Hur ser avsändar- och mottagaradresserna ut på lager 2 och 3?)

3. Beskriv hur kommunikation går till när en dator ska skicka ett IP-paket till en annan host som **ej finns** på det lokala nätverket. (Hur ser avsändar- och mottagaradresserna ut på lager 2 och 3?)

4. Ange vilka IPv4-adresser som är privata adresser (enligt RFC 1918)

5. Vad är skillnaden mellan adresserna 255.255.255.255 och 192.168.20.255? (På nätverk med standardmask /24.)

6. Ett nätverkskort har adressen 169.254.50.67 med nätmasken 255.255.0.0. Vad innebär detta?

7. Vad är IPv4-adressen till *localhost*?

8. Varför är det alltid 2 adresser i ett nätverk som ej kan användas som host-adresser?

9. Beskriv hur kommunikation går till när en dator ska skicka ett IP-paket till **alla andra** enheter på det lokala nätverket. (Hur ser avsändar- och mottagaradresserna ut på lager 2 och 3?)

10. Beskriv fälten *identifier* och *fragment offset* i IP-headern

11. Om flaggan **MF** är satt på ett paket vad betyder det?

12. Vad används fältet **TTL** till i IP-headern?

13. Vad används kommandot tracert (traceroute i Linux) till?

14. **Extra fördjupningsövning**: Om vi ska skapa ett nytt nätverk, varför kan det vara olämpligt generellt att använda IP-adresser i adressområdet 192.168.0.x eller 192.168.1.x?

IPv4 Del 2 – Laboration IP-headern

1. Starta en inspelning i Wireshark med filtret ”**icmp**”.

2. Pinga en adress på internet, t ex *www.sunet.se.*

3. Växla till Wireshark och hitta det första ICMP-meddelandet (echo request) från din dator. Markera paketet och studera IP-header.

   Kontrollera följande fält och förklara dem snabbt:
   Version: _____
   Header length: _____
   Total length: _____
   Time to Live: _____
   Header checksum: _____

   * Beroende på Wireshark- och Windows-version samt nätverkskorttyp - **om** IP-header-checksum noteras som inkorrekt eller är blankt på ett *utgående* paket, vad kan vara skälet till detta? (googla..)

   _____

4. Hitta det efterföljande paket med ”echo reply” och notera fältet TTL. Vilket värde har detta?

   _____

   Har detta någon relation till det TTL som det första paketet hade?

   _____

   Utifrån aktuellt värde som syns i svaret, går det att göra en gissning vilket TTL som avsändaren ursprungligen hade?

   _____

5. Ha en inspelning igång och använd ping tillsammans med växel **–i** för att sätta TTL till t ex 5 och försök pinga adress på internet.

   Notera i Wireshark om TTL går iväg med önskat värde.

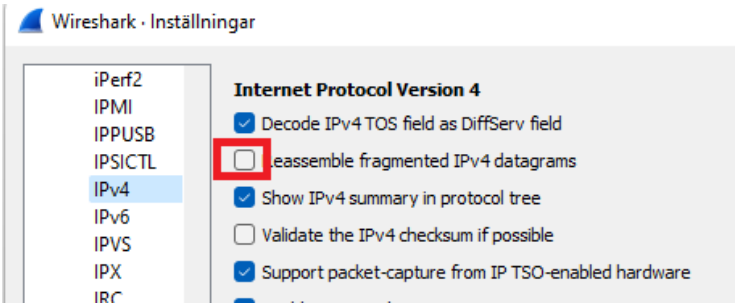
   Gör stegvis ökning och notera vilket TTL som krävs för att nå önskad plats.

   Påbörja ny inspelning i Wireshark och använd sedan kommando ”**tracert**” tillsammans med växel **–d** (ej namnupplösning) och gå mot lämplig adress på Internet.

   Kontrollera i Wireshark hur TTL-fälten ser ut på de paket som går iväg. Hur många paket syns med samma TTL innan ökning sker? _____

IPv4 Del 2 – Laboration IP-fragmentering

1. Ställ in i Wireshark – utifrån instruktion – att Wireshark *inte* skall göra egen visuell hopsamling av IP-fragment. (Redigera – Inställningar – Protocols – Ipv4 – Klicka ur "Reassemle fragmented IPv4 datagrams")



2. Starta en ny inspelning och sätt filter till ”**ip**”.

   Från kommandoprompt, kör:

   ping NÅGON-ADRESS –n 1 –l 30000
   (Någon adress kan vara din default gateway adress)
   (observera ovan att växel är lilla –n ger att endast skicka en ping-förfrågan för lättare studera utdatat. Och växeln -l (length) ange antalet bytes som ska skickas)

   Titta i Wireshark och notera det första paket som går iväg från din dator. I IP-header, expandera del för Flags och notera värdet på ”More fragments”. Är denna 0 eller 1?
   _____

3. Notera efterföljande paket (Fragmented IP protocol), studera fältet ”Fragment offset” i IP-header och notera att detta går uppåt utifrån mängd data som hittills gått iväg.

4. Kör nu samma kommando som ovan med addera växel –f (Do not Fragment). Vilket resultat får vi? _____

5. Varför är det generellt negativt med IP-fragmentering?
   _____
   _____

6. Vad är konceptet ”Path MTU Discovery” och hur fungerar det?
   _____
   _____
   _____
   _____
   _____

Öppna en webbläsare och anslut till någon eller några webbsidor. Via en kommandoprompt, kör kommando:

netsh int ipv4 show dest

Vad ser vi i listan?

_____

_____