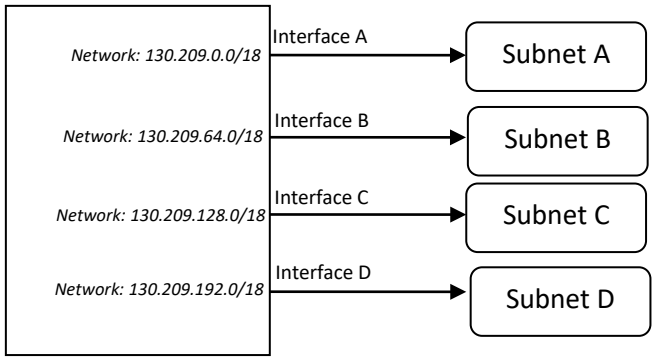
ANC4 Tutorial 2: Solutions

1. The TTL field of the header is decremented at every hop. As a result, the header checksum must be recomputed.
2. Layer 2 addresses contain no information about which network the device with a given address currently belongs to. When the destination network address can be extracted from the address of the target device, this allows "high-level" routers to reduce the problem of locating the target to one of locating the network to which it belongs.
3. A PMTU black hole will only throw away packets that exceed the relevant MTU. Packets below the MTU will pass without trouble. Thus short interactions between a client a server may succeed but as soon as there is any volume of data to transfer, packets will be discarded.
4. TCP MSS clamping can prevent a server from being supplied with optimistic information about the MTU the client expects. This is particularly a problem where the client LAN has a higher MTU than the ISP access link (e.g. PPPoE often has an MTU of 1492). When ICMP is blocked, this can resolve a PMTU black hole; even when ICMP is not blocked, it can prevent unnecessary cycles of PMTU discovery. Disadvantages include: ineffective on oversized UDP packets; slows down the router path, requiring intervention above layer 3; breaks the separation of layer 3 and layer 4 responsibilities at routers.
5. TCP clamping requires intervention above layer 3 which is usually seen as an unacceptable overhead in wire-speed routers. It is a strategy therefore most likely to be implemented close to the network edge. In common scenarios, such as web serving, most volume data goes server to client and therefore a MTU failure at the client end, caused by server data, is usually most likely and carries the greatest time penalty. Many web sites require opening of multiple TCP sessions so even one unnecessary RTT per session penalty is highly undesirable.
6. The host needs an IP address, directly-attached network mask and default gateway address.
7. It is not possible to direct a packet to a destination on a private network from a source outside it, unless the router has an existing port mapping for that destination.
8. A NAPT router does not use well-known port numbers (as used for TCP/UDP services) for mapping its private clients. However, a single private IP number can be reserved and associated with any such port number. That IP number can then be used as the address of a server on the private network. Only one address on a private network can be allocated to a given service. Thus the address associated with port number 80 can act as the private network's web server.
9. This is class B ($130 = 1000\ 0010_2$).
10. The mask for the network as a whole is 255.255.0.0. To divide it into 4 subnets a mask two bits longer is required, i.e. 255.255.192.0.0.
11. The design and table are as follows



Network	Mask	Interface	Gateway
130.209.0.0	255.255.192.0	A	A
130.289.64.0	255.255.192.0	B	B
130.209.128.0	255.255.192.0	C	C
130.209.192.0	255.255.192.0	D	D

Interface A will have a valid address on subnet A (e.g. 130.209.0.1) etc

12. Subnetting might be used to separate departments or functions in an organisation.
13. Yes but using default routing tables they will need to communicate via a router also attached to the LAN. This is because any destination not directly attached to the same subnet as the source will be automatically sent to the default gateway. Is it possible to add routes to the routing tables to avoid this.
14. The pseudo header is a attached to a TCP or UDP segment before it is passed to the IP layer. The pseudo-header includes source and destination IP addresses, a protocol number (6 for TCP) and a total byte count for the TCP/UDP segment. The pseudo header is not transmitted but is used by the IP layer to construct the IP header. It is however reconstructed at the destination and attached to the segment before it is passed to the receiving transport layer. The pseudo header is therefore the equivalent of a block of service parameters passed between the transport and IP layers. The TCP or UDP checksum is taken over segment and pseudo header together. This means that if an IP packet is mis-delivered by malfunctioning IP software but in a way which avoids detection by the IP header checksum, the pseudo-header constructed at the destination will be different from the original and the error will be detected by the TCP/UDP checksum.
15. Yes. For example set up a router as in Q9, but with interfaces C and D replaced with a single interface C_1, say. Then replace the two table entries for C and D with the following single entry.

130.209.128.0	255.255.128.0	C_1	C_1

16. Yes, a host-specific route will use a long mask (all ones). This will dominate any other matches for that host in any table in which it appears.
17. While an interface attached to an IP network must have at least one IP number, it is perfectly possible for it to have more than one. An example of a scenario where this might occur is that postulated in Q10 above. It is up to the IP layer to handle incoming and outgoing packets accordingly.
18. If the mask is 1 bit too long the directly attached route will be too restricted. Half the addresses in the local network will not be routed directly to their destinations but will be sent to the local gateway instead (via the default route).

    If the mask is too short the directly attached route will be too wide and some packets intended for other networks will erroneously match it. Instead of being sent to the local gateway, the host will try to delivering these packets itself by initiating an ARP (which will fail).