Entwerfe ein LAN 10.0.0.0/8 mit 10 PCs.  
Benenne alle PCs nach ihren IPv4 oder IPv6-Adressen und ordne sie zyklisch im Uhrzeigersinn nach ansteigender Adresse.

3 PCs sind nur IPv6-static konfiguriert in config/Interface oder Desktop/IP-Config  
mit IPv6 Address = Link Local Address ohne 1.Ziffer / 64

1.Firewall: der PC mit niedrigster IPv6-Adr empfängt nur Nachrichten (portunabhängig) von PC mit höchster IPv6-Adr:  
konfiguriere am PC mit niedrigster IPv6-Adr mit Desktop/IPv6Firewall:   
Action= ??, Protokoll= ?? (<>icmp), remoteIPv6= höchste existierende Host-IPv6-Adr / ??.  
ZEIGE Konsolen-Output von successful und failed pings und an diesem PC.

2 PCs konfiguriere beliebig aus 10.Knr.Knr.x/8  
2 PCs aus 10.2\*Knr.Knr.x/8 und   
2 PCs aus 10.2\*Knr.2\*Knr.x/8

2.Firewall: der PC mit höchster IPv4-Adr empfängt nur Pings von den 2 PCs mit den niedrigsten IPv4-Adr unter Verwendung von nur 1 Rule:  
- Action= ??, Prot= ??, RemoteIP= gleicher Adressanteil beider Adressen.0, WildcardMask= Negation der Subnetmask 255.255.255.0, die den gemeinsamen Adressanteil angibt  
ZEIGE Konsolen-Output eines einmaligen Broadcast-pings an diesem PC.

3.Firewall: Erstelle und ZEIGE einzig notwendige Allow-Rule mit der PC mit niedrigster IPv4-Adr keine Nachrichten vom PC mit zweitniedrigster IPv4-Adr empfängt.  
ZEIGE Konsolen-Output eines BC-pings an diesem PC.

Deine Abgabe beinhaltet alle mit GROßBUCHSTABEN geschriebenen Forderungen.

Erweiterte Kompetenz:  
STELLE alle Allow-Rules grafisch mit Draw Palette dar.