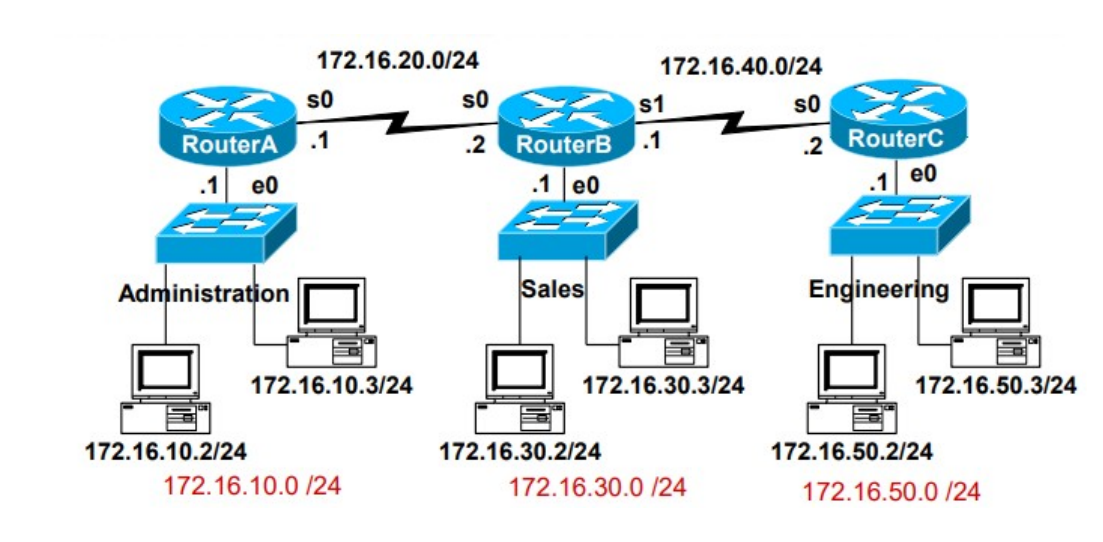
**Computer Engineering Department**

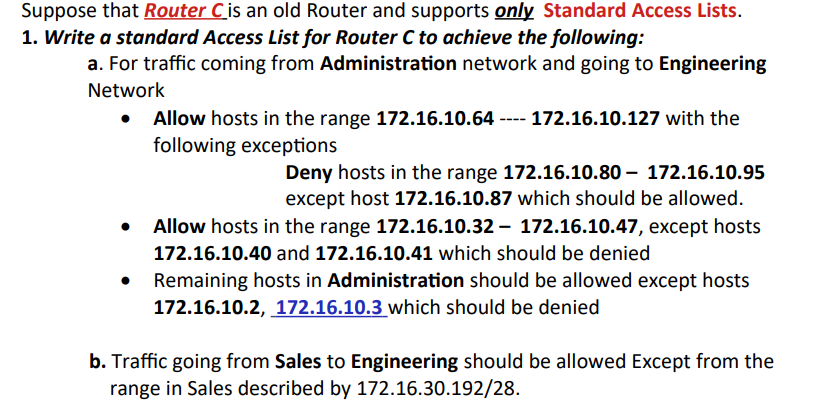
**Computer Networks 2 (10636455)**

**Access Lists – Assignment 1**

**Summer 2024**

****

**Part1:**

****

**Solution of Part1:**

**#access-list 1 permit 172.16.10.87 0.0.0.0** //**her I permit 172.16.10.87**

**#access-list 1 deny 172.16.10.80 0.0.0.15** //**here I deny 80-95**

**#access-list 1 permit 172.16.50.64 0.0.0.63** //**here I permit 64-127**

**#access-list 1 deny 172.16.10.40 0.0.0.1** //**here I deny 40 and 41**

**#access-list 1 permit 172.16.10.32 0.0.0.15** //**here I permit 32-47**

**#access-list 1 deny 172.16.10.2 0.0.0.1** //**here I deny 2 and 3**

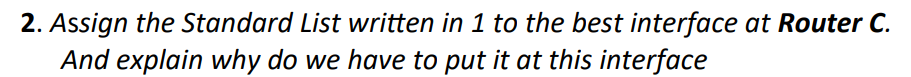
**#access-list 1 deny 172.16.30.192 0.0.0.15** //**here I deny 172.16.30.192**

**#access-list 10 permit any** // **here I permit all remaining addresses**

**from Administration and Sales to Engineering**.

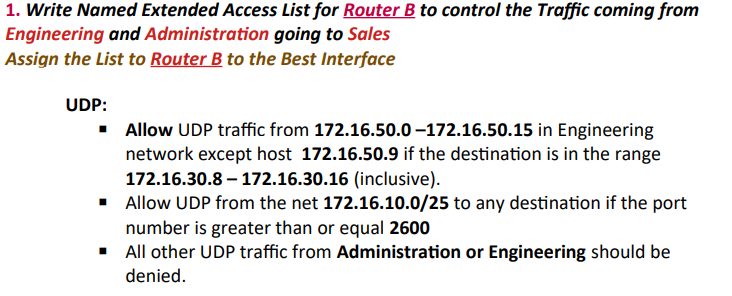
**#interface S0**

**#ip access\_group1 in .**

****

The best interface to apply the Standard Access Control List (ACL) from Step 1 is the **S0 interface**. Why? .We will place the access list on interface s0 on the input. This is because after checking the packets, if anything is rejected among them, the router will remove it before routing, rather than forwarding it and then discovering that it was rejected (based on the access list placed on the output).This improves the overall efficiency and performance of the router.

**Part2.1:**



**Solution of Part2.1:**

**#ip access\_list extended ENG\_ADM\_TO\_SAL**

**#deny UDP host 172.16.50.9 172.16.30.8 0.0.0.7 // deny t host 172.16.50.9 if the destination is in the range 172.16.30.8 – 172.16.30.16**

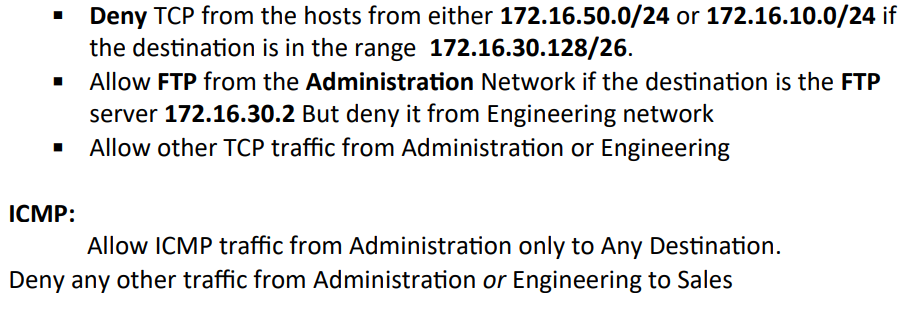
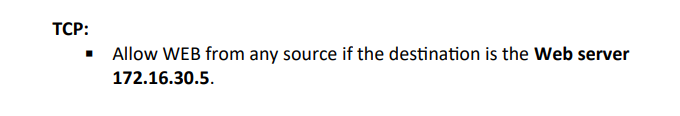
**#permit UDP 172.16.50.0 0.0.0.15 172.16.30.8 0.0.0.7 // Allow UDP traffic from 172.16.50.0 –172.16.50.15 in Engineering network**

**#permit UDP 172.16.10.0 0.0.0.127 any gt 2599 //** **Allow UDP from the net 172.16.10.0/25 to any destination if the port number is greater than or equal 2600**

**#deny any any //** **All other UDP traffic from Administration or Engineering should be denied.**

**#interface e0**

**#ip access\_group in**



**#ip access\_list extended ENG\_ADM\_TO\_SAL**

**#permit TCP any 172.16.30.5 0.0.0.0 eq 80 // Allow WEB from any source if the destination is the Web server 172.16.30.5**

**#deny TCP 172.16.50.0 0.0.0.255 172.16.30.128 0.0.0.63**

**#deny TCP 172.16.10.0 0.0.0.255 172.16.30.128 0.0.0.63**

**//Deny TCP from the hosts from either 172.16.50.0/24 or 172.16.10.0/24 if the destination is in the range 172.16.30.128/26.**

**permit TCP 172.16.10.0 0.0.0.255 host 172.16.30.2 eq 21#**

**deny TCP 172.16.50.0 0.0.0.255 host 172.16.30.2 eq 21#**

**permit TCP 172.16.10.0 0.0.0.255 host 172.16.30.2 eq 20#**

**deny TCP 172.16.50.0 0.0.0.255 host 172.16.30.2 eq 20#**

**//Allow FTP from the Administration Network if the destination is the FTP server 172.16.30.2 But deny it from Engineering network**

**permit TCP 172.16.10.0 0.0.0.255 any #**

**#permit TCP 172.16.50.0 0.0.0.255 any**

**//Allow other TCP traffic from Administration or Engineering**

**#permit ICMP 172.16.10.0 0.0.0.255 any // Allow ICMP traffic from Administration only to Any Destination**

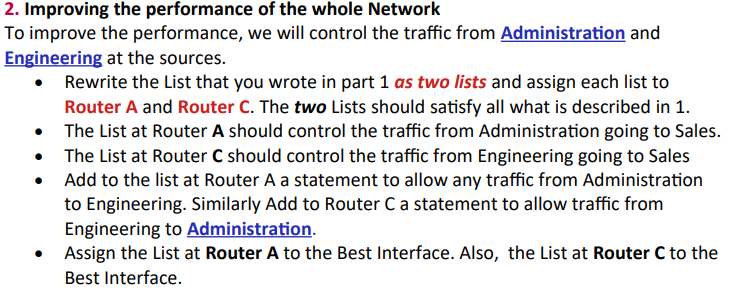
**deny ip 172.16.10.0 0.0.0.255 172.16.30.0 0.0.0.255#**

**deny ip 172.16.50.0 0.0.0.255 172.16.30.0 0.0.0.255#**

**// Deny any other traffic from Administration or Engineering to Sales**

**#interface e0**

**#ip access\_group out**.



**Solution of Part2.1:**

**Access list on ROUTER A --**

**#ip access-list extended ADMIN\_TO\_SALE**

**#permit UDP 172.16.10.0 0.0.0.127 any gt 2599** //**Allow UDP from the net 172.16.10.0/25 to any destination if the port number is greater than or equal 2600**

**#permit TCP any host 172.16.30.5 eq 80** //**Allow WEB from any source if the destination is the Web server 172.16.30.5**

**#deny TCP 172.16.10.0 0.0.0.255 172.16.30.128 0.0.0.63 //Deny TCP from the host 172.16.10.0/24 if the destination is in the range 172.16.30.128/26**

**#permit TCP 172.16.10.0 0.0.0.255 host 172.16.30.2 eq 21**

**#permit TCP 172.16.10.0 0.0.0.255 host 172.16.30.2 eq 20** //**Allow FTP from the Administration Network if the destination is the FTP**

**#permit ICMP 172.16.10.0 0.0.0.255 any //Allow ICMP traffic from Administration only to Any Destination**.

**#deny UDP 172.16.10.0 0.0.0.255 172.16.30.0 0.0.0.255** //**All other UDP traffic from Administration should be denied**.

**#permit TCP 172.16.10.0 0.0.0.255 172.16.30.0 0.0.0.255**// **Allow other TCP traffic from Administration or Engineering**

**#deny ip 172.16.10.0 0.0.0.255 172.16.30.0 0.0.0.255**//**Deny any other traffic** **from Administration to Sales**

**#permit ip 172.16.10.0 0.0.0.255 172.16.50.0 0.0.0.255 //Allow all traffic from Administration to Engineering**

**#interface e0**

**#ip access\_group out**

**-Access list on ROUTER C-**

**#ip access-list extended ENG\_TO\_SAL**

**# deny UDP host 172.16.50.9 172.16.30.8 0.0.0.7 // deny 172.16.50.9 if the destination is in the range 172.16.30.8 – 172.16.30.16.**

**#permit UDP 172.16.50.0 0.0.0.15 172.16.30.8 0.0.0.7 // Allow UDP traffic from 172.16.50.0 –172.16.50.15 in Engineering network if the destination is in the range 172.16.30.8 – 172.16.30.16 .**

**#permit TCP any host 172.16.30.5 eq 80 //Allow WEB from any source if the destination is the Web server 172.16.30.5.**

**#deny TCP 172.16.50.0 0.0.0.255 172.16.30.128 0.0.0.63 // Deny TCP from the hosts from 172.16.50.0/24 if the destination is in the range 172.16.30.128/26.**

**#deny TCP 172.16.50.0 0.0.0.255 host 172.16.30.2 eq 21**

**deny TCP 172.16.50.0 0.0.0.255 host 172.16.30.2 eq 20 //Deny FTP from the Engineering Network if the destination is the FTP server 172.16.30.2**

**#permit TCP 172.16.50.0 0.0.0.255 any //Allow other TCP traffic from Engineering to sales**

**# deny ip 172.16.50.0 0.0.0.255 172.16.30.0 0.0.0.255 //Deny any other traffic from Administration or Engineering to Sales**

**#permit ip 172.16.50.0 0.0.0.255 172.16.10.0 0.0.0.255 //Allow all traffic from Engineering to Administration**

**#interface e0**

**#ip access\_group out**