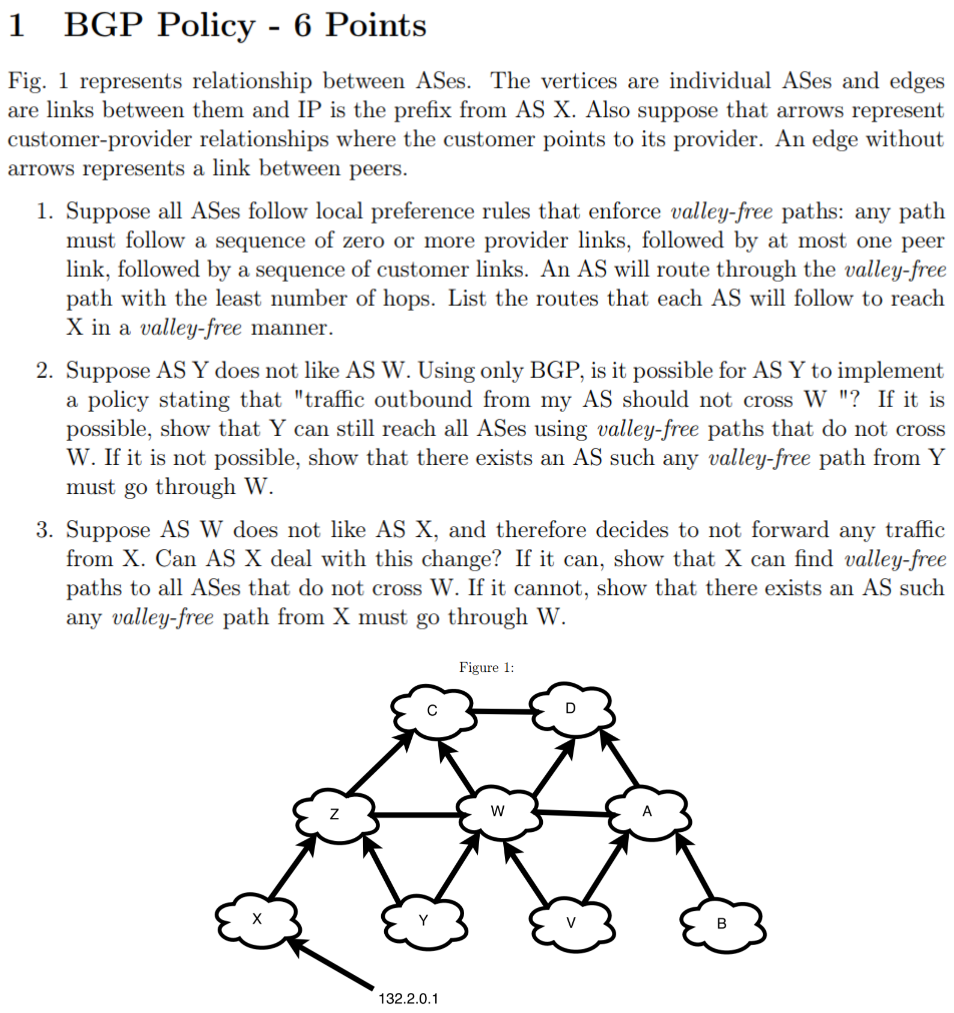
CS438 Assignment 4

04/27/2023

Wang, Jie [jiew5]
Wu, Jiaxin [jiaxin19]

1. BGP Policy



1 BGP Policy - 6 Points

Fig. 1 represents relationship between ASes. The vertices are individual ASes and edges are links between them and IP is the prefix from AS X. Also suppose that arrows represent customer-provider relationships where the customer points to its provider. An edge without arrows represents a link between peers.

1. Suppose all ASes follow local preference rules that enforce *valley-free* paths: any path must follow a sequence of zero or more provider links, followed by at most one peer link, followed by a sequence of customer links. An AS will route through the *valley-free* path with the least number of hops. List the routes that each AS will follow to reach X in a *valley-free* manner.
2. Suppose AS Y does not like AS W. Using only BGP, is it possible for AS Y to implement a policy stating that "traffic outbound from my AS should not cross W "? If it is possible, show that Y can still reach all ASes using *valley-free* paths that do not cross W. If it is not possible, show that there exists an AS such any *valley-free* path from Y must go through W.
3. Suppose AS W does not like AS X, and therefore decides to not forward any traffic from X. Can AS X deal with this change? If it can, show that X can find *valley-free* paths to all ASes that do not cross W. If it cannot, show that there exists an AS such any *valley-free* path from X must go through W.

Figure 1:

1. ASes to X:

- A: A, D, C, Z, X
- B: B, A, D, C, Z, X
- C: C, Z ,X
- D: D, C, Z, X
- V: V, W, Z, X
- W: W, Z, X
- X: X
- Y: Y, Z, X
- Z: Z, X

2. Y hate W

Yes, it is possible.

Y can still reach all ASes by the following paths:

A: Y, Z, C, D, A
B: Y, Z, C, D, A, B
C: Y, Z, C
D: Y, Z, C, D
V: Y, Z, C, D, A, V
X: Y, Z, X
Y: Y
Z: Y, Z

3. W hate X

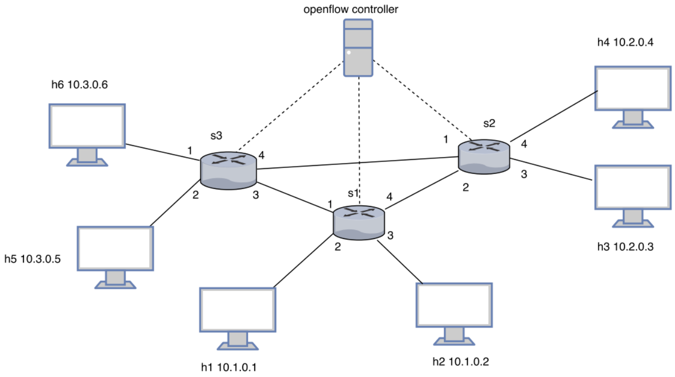
Yes, it is possible.

X can still reach all ASes by the following paths:
A: X, Z, C, D, A
B: X, Z, C, D, A, B
C: X, Z, C
D: X, Z, C, D
V: X, Z, C, D, A, V
X: X
Y: X, Z, Y
Z: X, Z

2. SDNs

Consider the SDN OpenFlow network shown below in Fig. 2. Suppose we want switch s2 to function as a firewall. Specify the flow table in s2 that implements the following firewall behaviors. Specify a different flow table for each of the four firewalling behaviors below. The flow table should only consider delivery of datagrams destined to h3 and h4. You do not need to specify the forwarding behavior in s2 that forwards traffic to other routers. The flow table should show the matching rule and the action taken.

Figure 2:



1. Only traffic arriving from hosts h2 and h5 should be delivered to hosts h3 or h4.
2. Only TCP traffic is allowed to be delivered to hosts h3 or h4.(i.e., that UDP traffic is blocked.)
3. Only traffic destined to h4 is to be delivered (i.e., all traffic to h3 is blocked.)
4. Only UDP traffic from h6 and destined to h3 is to be delivered. All other traffic is blocked.

Referring to Openflow docs: we need to specify:

- **nw_proto**: where 6 denotes TCP, 17 denotes UDP
- **nw_src**
- **nw_dst**

In the matching rule

1. h2&h5 to h3&h4

- Matching rule: if (source ip = 10.1.0.2 or 10.3.0.5) and destination ip = 10.2.0.3
  - Action: forward to h3
  - Else: drop
- Matching rule: if (source ip = 10.1.0.2 or 10.3.0.5) and destination ip = 10.2.0.4
  - Action: forward to h4
  - Else: drop

2. Only TCP to h3&h4

- Matching rule: IP protocol attribute is TCP and destination ip = 10.2.0.3
  - if (nw_proto == 6 && nw_dst == 10.2.0.3)
  - Action: forward(h3)
- Matching rule: IP protocol attribute is TCP and destination ip = 10.2.0.4
  - if (nw_proto == 6 && nw_dst == 10.2.0.4)
  - Action: forward(h4)

3. Block h3 only

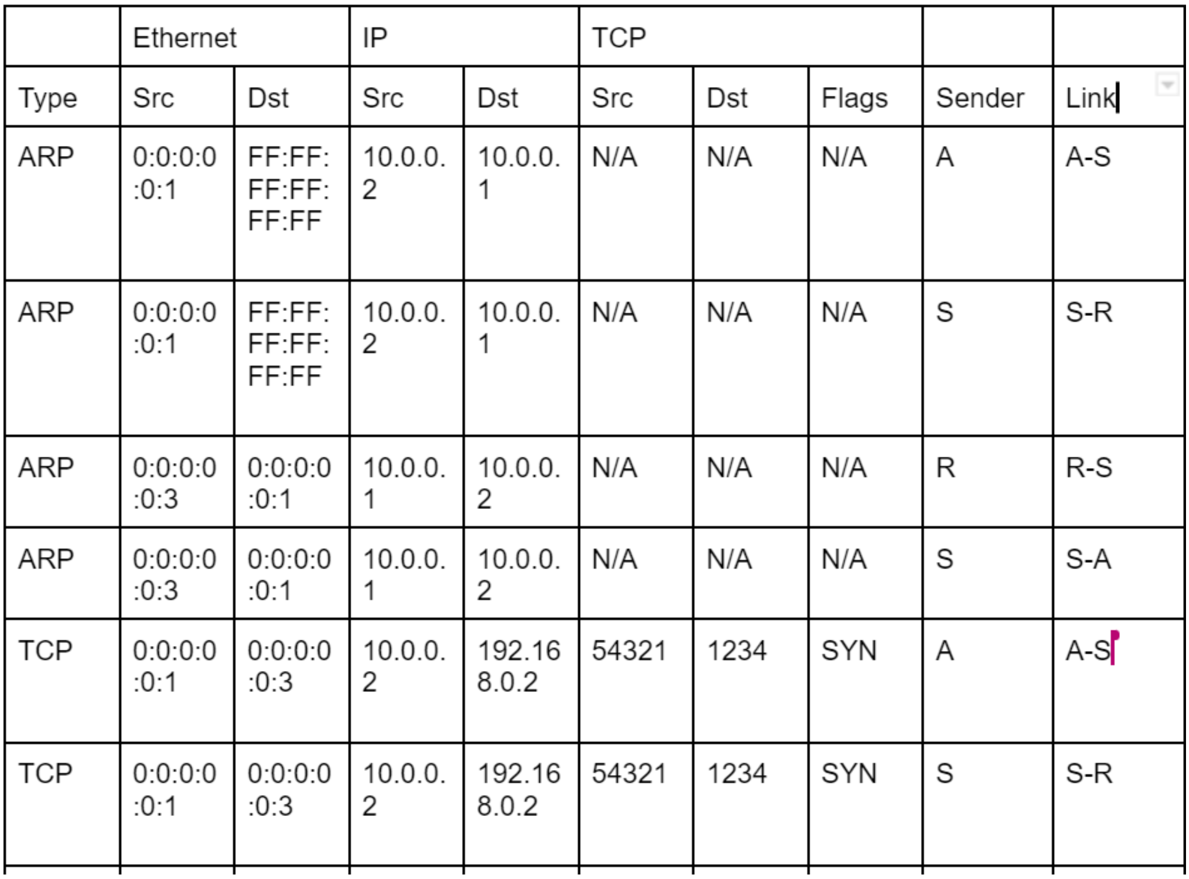
- Matching rule: if destination ip = 10.2.0.4
    - Action: forward(h4)

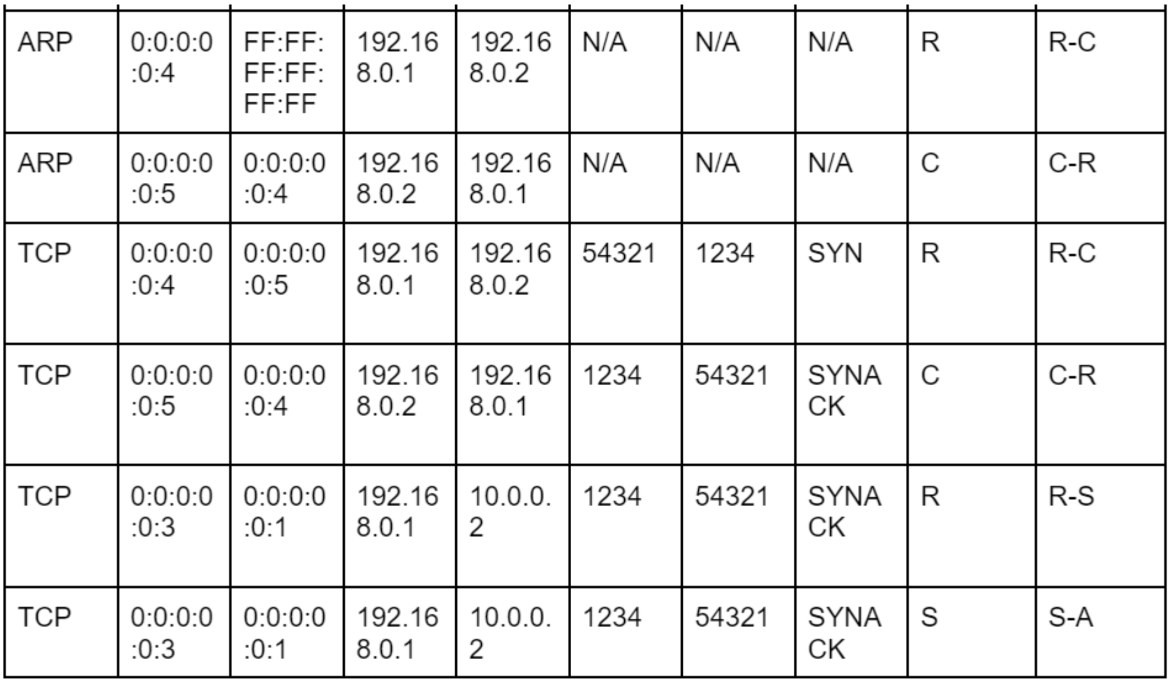
4. h6-UDP-h3 only

- Matching rule:
    - source ip = 10.3.0.6 , destination ip = 10.2.0.3 and P protocol attribute is UDP
    - if (nw_proto == 17 && nw_src == 10.3.0.6 && nw_dst == 10.2.0.3)
    - Action: forward(h3)

> Citation:
>
> Campuswire: TCP or UDP would be specified by the IP prot, or nw_proto

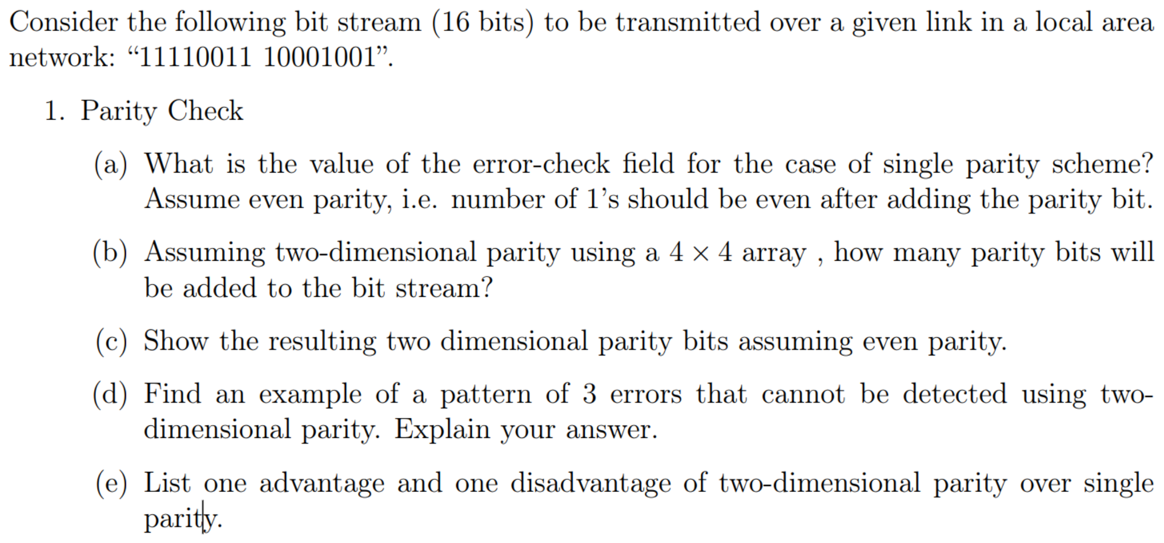
3. Synthesis





	Ethernet		IP		TCP				
Type	Src	Dst	Src	Dst	Src	Dst	Flags	Sender	Link
ARP	0:0:0:0:0:1	FF:FF:FF:FF:FF:FF	10.0.0.2	10.0.0.1	N/A	N/A	N/A	A	A-S
ARP	0:0:0:0:0:1	FF:FF:FF:FF:FF:FF	10.0.0.2	10.0.0.1	N/A	N/A	N/A	S	S-R
ARP	0:0:0:0:0:3	0:0:0:0:0:1	10.0.0.1	10.0.0.2	N/A	N/A	N/A	R	R-S
ARP	0:0:0:0:0:3	0:0:0:0:0:1	10.0.0.1	10.0.0.2	N/A	N/A	N/A	S	S-A
TCP	0:0:0:0:0:1	0:0:0:0:0:3	10.0.0.2	192.168.0.2	54321	1234	SYN	A	A-S
TCP	0:0:0:0:0:1	0:0:0:0:0:3	10.0.0.2	192.168.0.2	54321	1234	SYN	S	S-R
ARP	0:0:0:0:0:4	FF:FF:FF:FF:FF:FF	192.168.0.1	192.168.0.2	N/A	N/A	N/A	R	R-C
ARP	0:0:0:0:0:5	0:0:0:0:0:4	192.168.0.2	192.168.0.1	N/A	N/A	N/A	C	C-R
TCP	0:0:0:0:0:4	0:0:0:0:0:5	192.168.0.1	192.168.0.2	54321	1234	SYN	R	R-C
TCP	0:0:0:0:0:5	0:0:0:0:0:4	192.168.0.2	192.168.0.1	1234	54321	SYNACK	C	C-R
TCP	0:0:0:0:0:3	0:0:0:0:0:1	192.168.0.1	10.0.0.2	1234	54321	SYNACK	R	R-S
TCP	0:0:0:0:0:3	0:0:0:0:0:1	192.168.0.1	10.0.0.2	1234	54321	SYNACK	S	S-A

4. Error Detection



Consider the following bit stream (16 bits) to be transmitted over a given link in a local area network: “11110011 10001001”.

1. Parity Check

   (a) What is the value of the error-check field for the case of single parity scheme? Assume even parity, i.e. number of 1’s should be even after adding the parity bit.

   (b) Assuming two-dimensional parity using a 4 × 4 array , how many parity bits will be added to the bit stream?

   (c) Show the resulting two dimensional parity bits assuming even parity.

   (d) Find an example of a pattern of 3 errors that cannot be detected using two-dimensional parity. Explain your answer.

   (e) List one advantage and one disadvantage of two-dimensional parity over single parity.

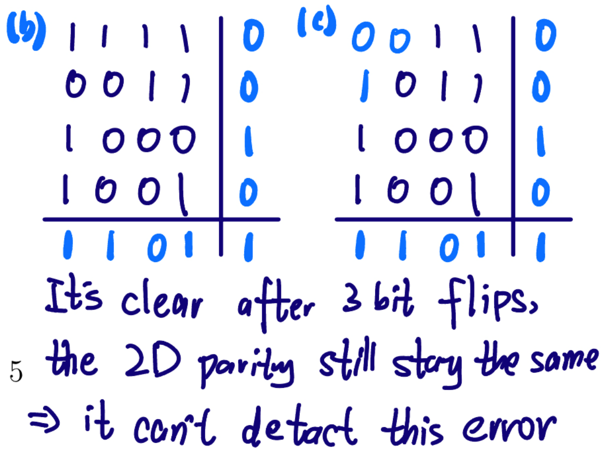
1. Parity Check

(a) 1

(b) 4+4 +1 = 9

(c) & (d)array:

####



(b)

1	1	1	1	0
0	0	1	1	0
1	0	0	0	1
1	0	0	1	0
1	1	0	1	1

(c)

0	0	1	1	0
1	0	1	1	0
1	0	0	0	1
1	0	0	1	0
1	1	0	1	1

It's clear after 3 bit flips,

5 the 2D parity still stay the same

⇒ it can't detect this error

(e)

- **Advantage:** 2D parity can self-detect and correct single-bit errors. It is more powerful
- **Disadvantage:** 2D parity requires more parity bits, increasing the overhead and space complexity

2. Cyclic Redundancy Checksum

The given bit stream is to be protected by a CRC code using the CRC-8 generator "100100110".

(a) Calculate the CRC bits using modulo 2 long division. Show the steps of your calculation.

(b) What is the resulting bit stream to be transmitted?

(c) How does the receiver know if an error has occurred in the transmitted bit stream?

(d) Suppose that the leftmost bit of the transmitted bit stream is inverted due to noise on the transmission link, what is the result of the receiver's CRC check? Show the steps of your calculation.

(a) Shown below:

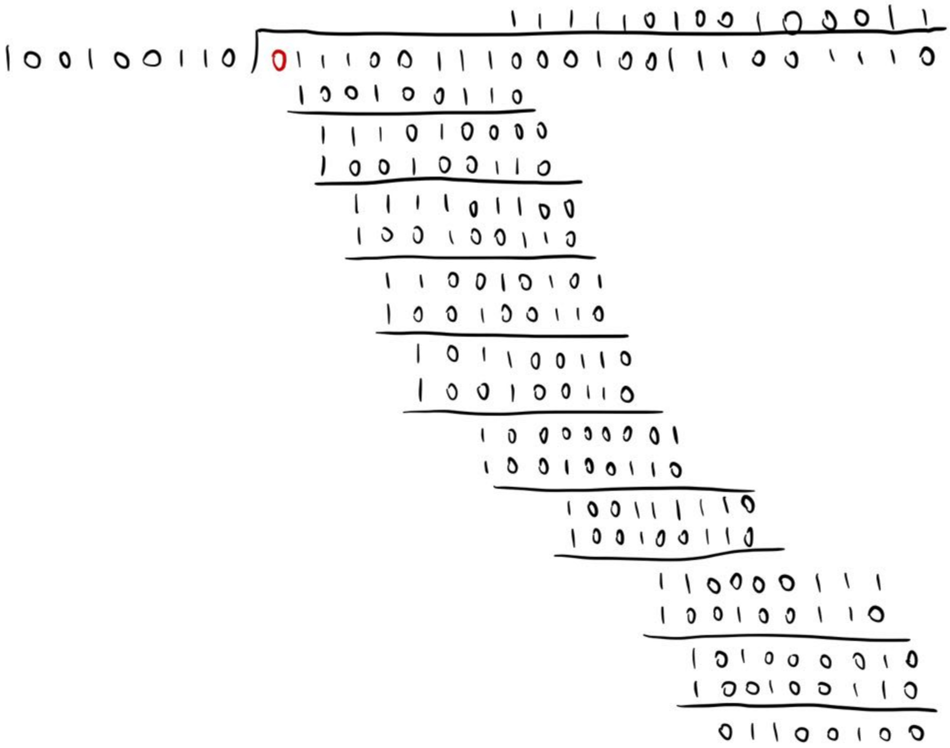
```
                   1110110001101101
100100110 /111100111000100100000000
           100100110
           ---------
           0110000010
            100100110
            ---------
             101001000
             100100110
             ---------
               1101110
               000000001
               ---------
               110111001
               100100110
               ---------
                100111110
                100100110
                ---------
                    110000100
                    100100110
                    ---------
                     101000100
                     100100110
                     ---------
                       110001000
                       100100110
                       ---------
                        101011100
                        100100110
                        ---------
                          111101000
                          100100110
                          ---------
                           11001110
```

(b) 1111 0011 1000 1001 1100 1110

"1111 0011 1000 1001" + 8 CRC bit

(c) The receiver divides the received bit stream <D,R> by G using modulo 2 long division. If the remainder is not zero, error is detected.

(d) Shown below



```
                   111110100100011
          ________________________
100100110)011100111000100111001110
           100100110
           ---------
            111010000
            100100110
            ---------
             111101100
             100100110
             ---------
              110010101
              100100110
              ---------
               101100110
               100100110
               ---------
                 100000001
                 100100110
                 ---------
                    100111110
                    100100110
                    ---------
                        110000111
                        100100110
                        ---------
                         101000010
                         100100110
                         ---------
                          011000100
```

3. Checksum

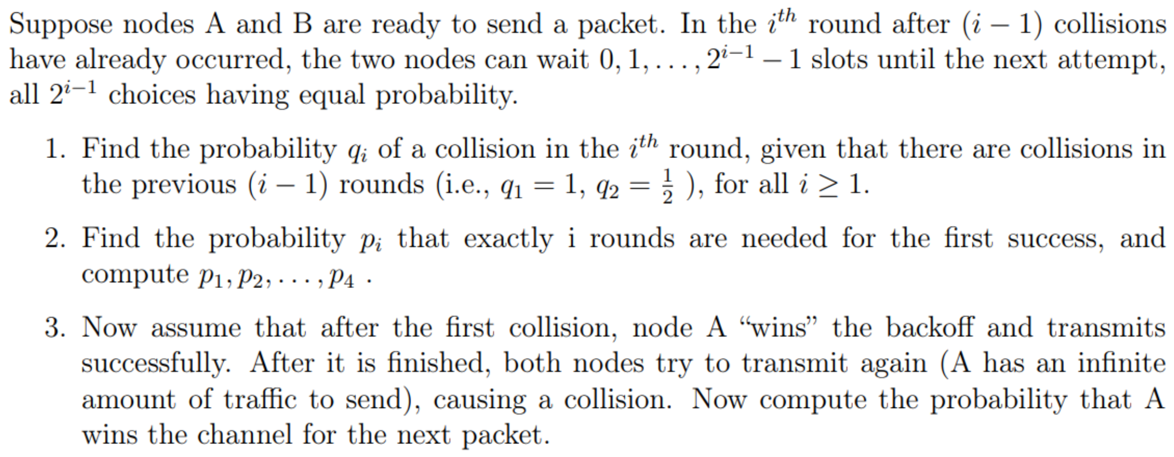
0x7EFF = 0111 1110 1111 1111
0xAAC8 = 1010 1010 1100 1000
0xEC05 = 1110 1100 0000 0101
0x7EFF + 0xAAC8 = 1 0010 1001 1100 0111
Wrap around:

0x7EFF+0xAAC8= 0010 1001 1100 1000
0x7EFF+0xAAC8+0xEC05=1 0001 0101 1100 1101
Wrap around:

0x7EFF+0xAAC8+0xEC05=0001 0101 1100 1110

1’s complement sum =1110 1010 0011 0001

5. Channel Contention



Suppose nodes A and B are ready to send a packet. In the i^{th} round after $(i-1)$ collisions have already occurred, the two nodes can wait $0, 1, \ldots, 2^{i-1}-1$ slots until the next attempt, all 2^{i-1} choices having equal probability.

1. Find the probability q_i of a collision in the i^{th} round, given that there are collisions in the previous $(i-1)$ rounds (i.e., $q_1 = 1$, $q_2 = \frac{1}{2}$), for all $i \geq 1$.
2. Find the probability p_i that exactly i rounds are needed for the first success, and compute $p_1, p_2, \ldots, p_4$.
3. Now assume that after the first collision, node A "wins" the backoff and transmits successfully. After it is finished, both nodes try to transmit again (A has an infinite amount of traffic to send), causing a collision. Now compute the probability that A wins the channel for the next packet.

1.

At round i, each node can wait $0, 1, \ldots, 2^{(i-1)} - 1$ slots, all 2^{i-1} choices having $\frac{1}{2^{i-1}}$ probability. A collision happens in i-th round if A and B both choose to wait k slots, where $k = 0, 1, \ldots, 2^{i-1} - 1$, the probability is $2^{i-1} * \frac{1}{2^{i-1}} * \frac{1}{2^{i-1}} = \frac{1}{2^{i-1}}$.

2.

The first success happens at the exactly i-th rounds if there are collisions in the first (i-1) rounds and success in the i-th round.

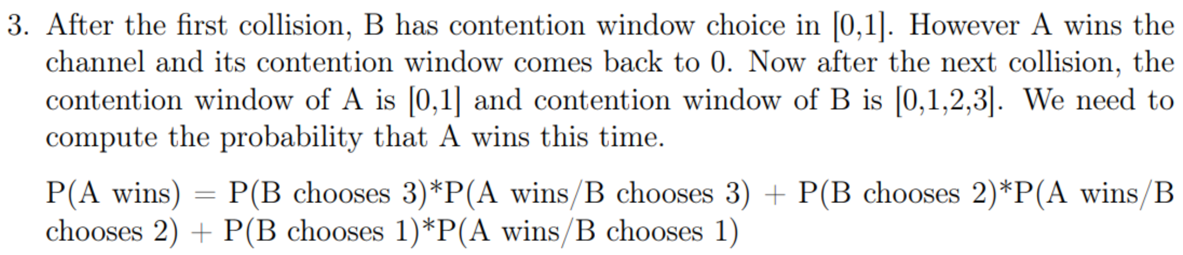
$$p1 = 1 - \frac{1}{2^{1-1}} = 0 \tag{1}$$

$$p2 = \frac{1}{2^{1-1}} * (1 - \frac{1}{2^{2-1}}) = \frac{1}{2} \tag{2}$$

$$p3 = \frac{1}{2^{1-1}} * \frac{1}{2^{2-1}} * (1 - \frac{1}{2^{3-1}}) = \frac{3}{8} \tag{3}$$

$$p3 = \frac{1}{2^{1-1}} * \frac{1}{2^{2-1}} * \frac{1}{2^{3-1}} * (1 - \frac{1}{2^{4-1}}) = \frac{7}{64} \tag{4}$$

3.



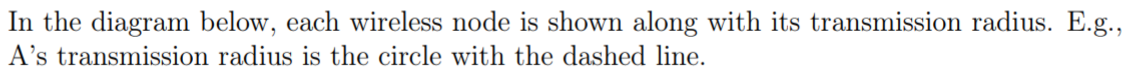
3. After the first collision, B has contention window choice in [0,1]. However A wins the channel and its contention window comes back to 0. Now after the next collision, the contention window of A is [0,1] and contention window of B is [0,1,2,3]. We need to compute the probability that A wins this time.

   P(A wins) = P(B chooses 3)*P(A wins/B chooses 3) + P(B chooses 2)*P(A wins/B chooses 2) + P(B chooses 1)*P(A wins/B chooses 1)

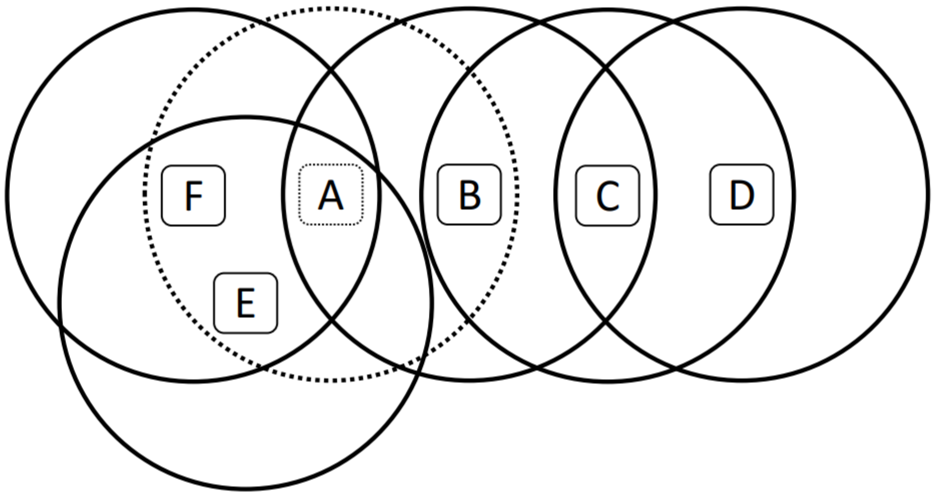
$$P(Awins) = 1/4 * 1 + 1/4 * 1 + 1.4 * 1/2$$

$$P(Awins) = 5/8$$

6. Wireless



In the diagram below, each wireless node is shown along with its transmission radius. E.g., A's transmission radius is the circle with the dashed line.



1. Hidden Terminals

F(A)B, A(B)C, B(C)D, E(A)B

2. Collision Avoidance

No, because F or E may be send RTS to A at the same time, and a collision will occur.

3. ACK is necessary

For wireless network, the unstable environment causes a lot of inferences to the signal.

- Node A sends an ACK message to confirm that it has successfully received the packet.
- If node B doesn't receive an ACK message within a certain timeframe, it will assume that the packet is lost and resend the packet.
- So it is necessary to send an ACK message to ensure reliable wireless transfer.

4. SINR of C at D

(a) noise power at D = 0

According to the *decreased signal strength* formula from course,

$$p_{R_X} = \alpha * \frac{P_{T_x}}{d^2} \tag{5}$$

Suppose the received signal power at D is P,

- then the inference from A at D is $\frac{P}{3^2} = \frac{P}{9}$.

  Then by formula above, $SINR = \frac{P}{P/9} = 9$.

(b)

Suppose the received signal power at D is P, then the noise power at D is P/18

then, $SINR = P \div (P/18 + P/9) = 6$

5. BER vs SNR curve

(a) SNR = 12dB, which modulation scheme maximize bit rate?

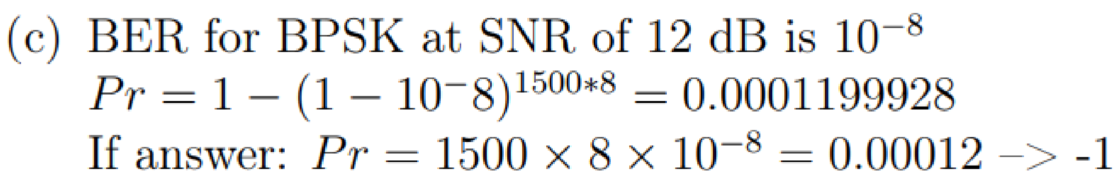
BPSK should be used since it is the only scheme with BER less than 10^{-6} when SNR is 12.

(b) If bandwidth = 10Mhz, bit rate = ? under (a)

Since BPSK transfers 1 bit per symbol,

the bit rate = bandwidth * bits/symbol = 10MHz * 1 = **10Mbps**

(c) BER for BPSK



(c) BER for BPSK at SNR of 12 dB is 10^{-8}

$Pr = 1 - (1 - 10^{-}8)^{1500*8} = 0.0001199928$

If answer: $Pr = 1500 \times 8 \times 10^{-8} = 0.00012$ −> -1