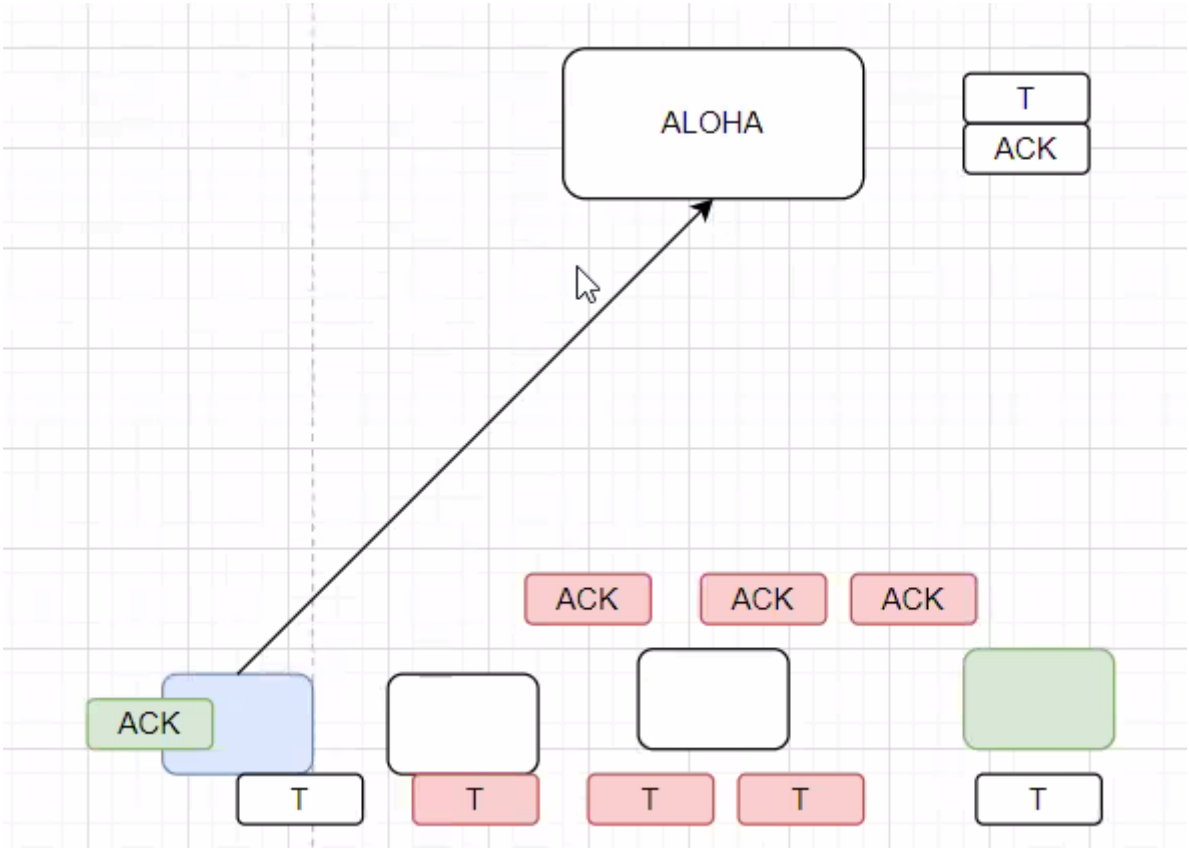
Apunte #2: Clase del 1-9-23

Instituto Tecnológico de Costa Rica. Escuela de Ingeniería en Computación. Redes - IC-7602. Grupo 2. Profesor: Gerardo Nereo Campos Araya Estudiante: Daniel Araya Sambucci - 2020207809 Fecha de entrega: 8/9/23

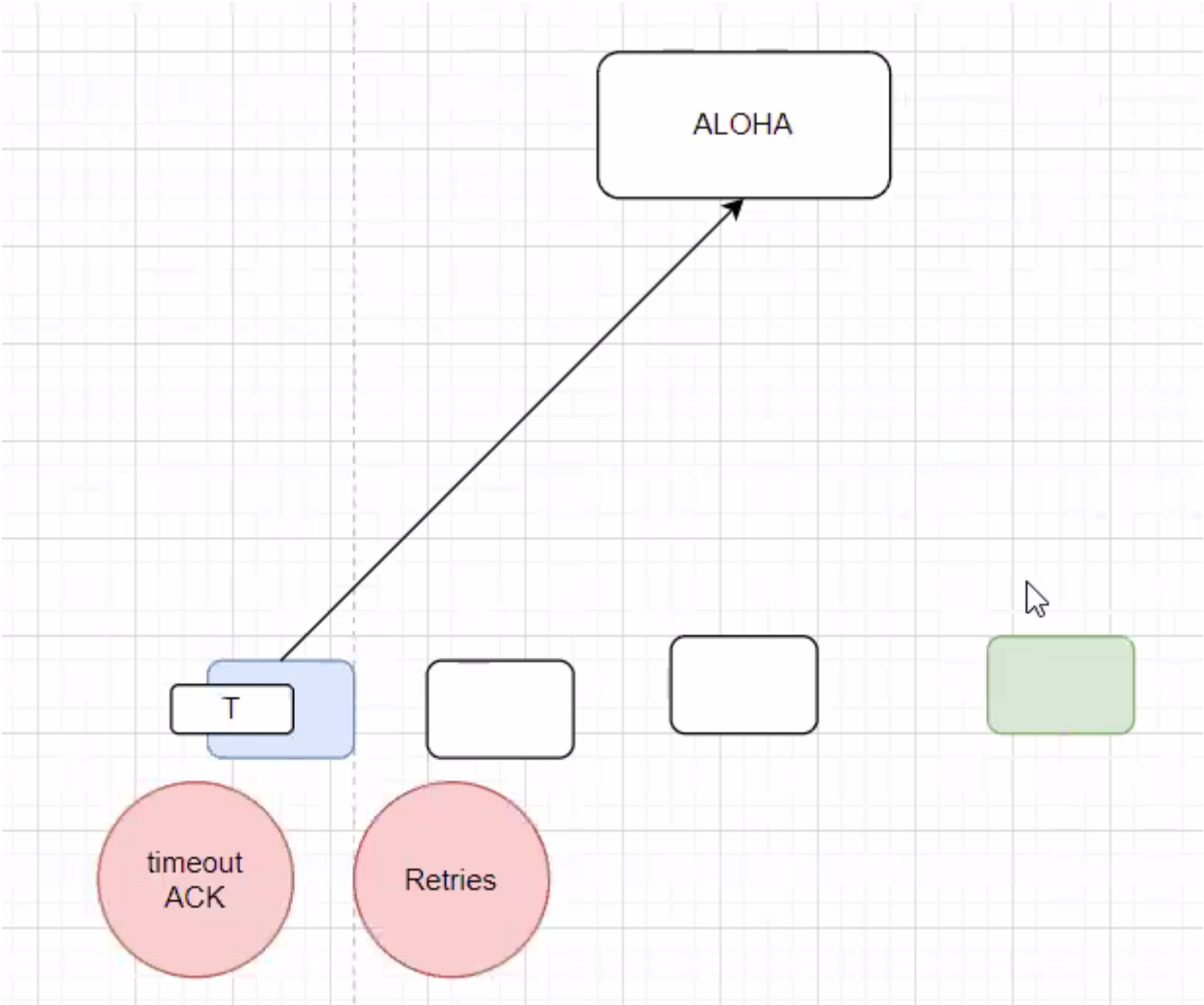
Repaso clase martes

ALOHA Puro

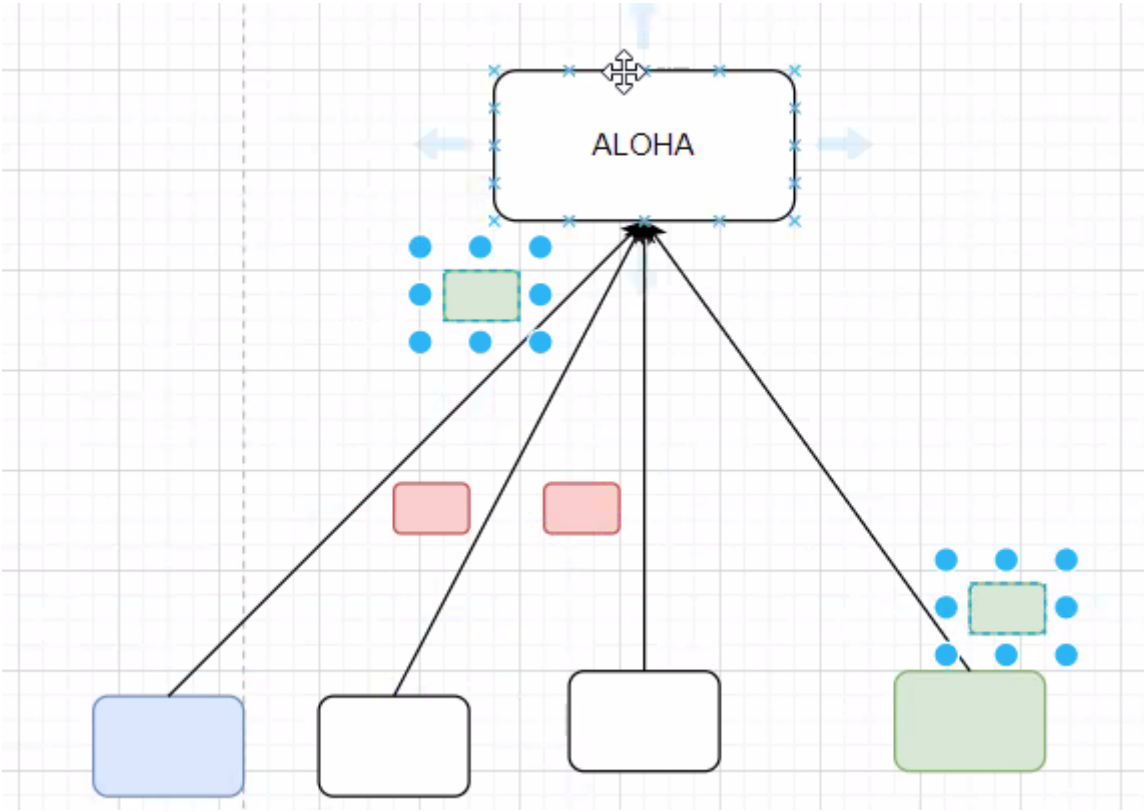
Cuando se tiene más de una entidad accediendo al recurso compartido, se debe implementar un algoritmo que gobierne cómo usar el recurso compartido. Si esto no se implementa, entonces habrá colisiones que provocarán una destrucción. Una destrucción es una deformación del espectro al grado de que será irreconocible la información que se está enviando, lo que podría verse como la destrucción de la información.



Cuando una estación quiere transmitir, envía la información al satélite. Al satélite recibir la trama, usa la difusión para enviar la trama a las demás estaciones. En el mejor de los casos, la estación que envía la trama la recibe. Las estaciones que reciben la trama y no la estaban esperando la ignoran. La estación objetivo la recibe. La estación objetivo entonces manda un ACK al satélite, el satélite va a difundir la trama del ACK y ocurre lo mismo para la estación objetivo. En una situación casi perfecta, la estación manda la trama al satélite y el satélite al difundir, logró que la trama llegara a la estación emisora, pero no llegó a la objetivo. Esto lo que dirá es que en la estación emisora se activa un timeout para esperar por el ACK. Como este timeout expira, entonces la estación volverá a enviar la trama y el satélite volverá a hacer la difusión. Esto ocurre hasta que la estación base objetivo recibe la trama, envíe el ACK y sea recibido por la estación base emisora.

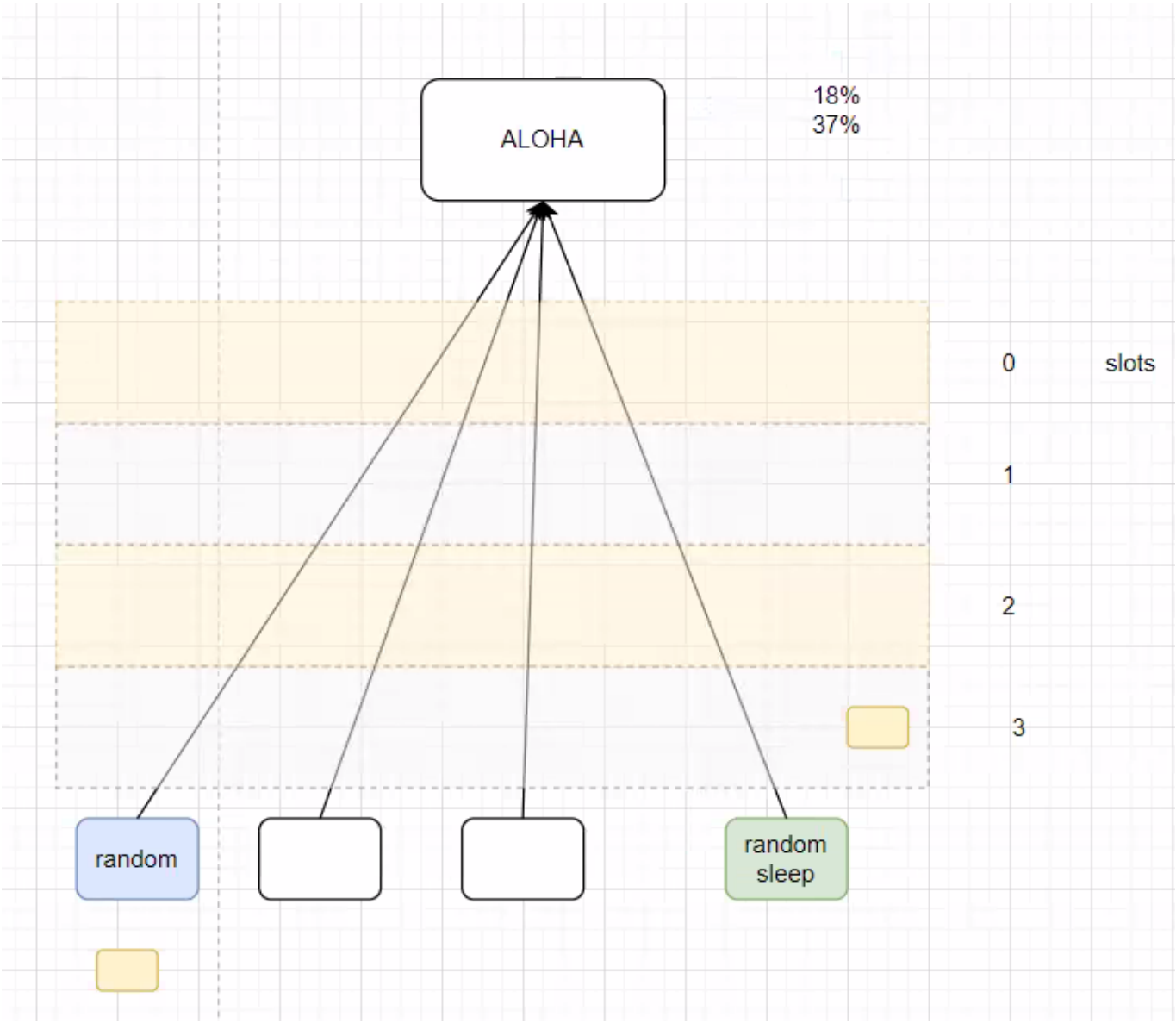


Si el ACK no llega al satélite, entonces nuevamente expira el timeout y se repite el ciclo hasta que se reciba el paquete. Esto ocurrirá hasta que expiren todos los timeout y se acaben los retries.



En un mundo algo más imperfecto, varias estaciones envíen tramas a la vez. Cuando dos o más estaciones envían tramas simultáneas, se da una colisión. Es altamente probable que las que enviaron en distintos tiempos sus tramas tengan un éxito en la transmisión. Al tener solo un 18% de éxito de transmisión el ALOHA, entonces para mejorar este porcentaje se usará un esquema ranurado.

ALOHA Ranurado

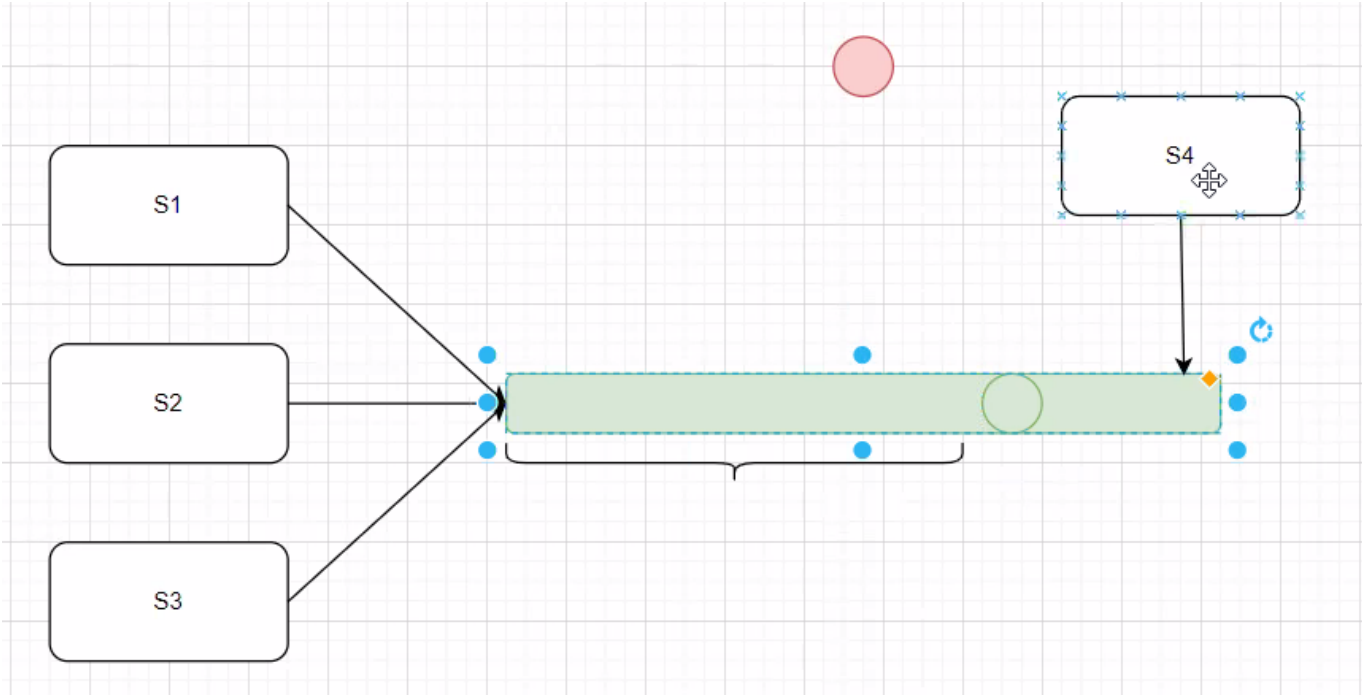


Se usan ranuras de tiempo en las cuales las tramas se pueden enviar. Los slots definen la forma en el que se podrán enviar las tramas. Para poder transmitir, las estaciones deben esperarse al inicio del slot. Si dos estaciones transmiten a la vez, entonces es altamente probable que se destruyan las tramas. Si esto ocurre, entonces se realiza un backoff. Se genera un número random para posteriormente hacer un sleep. De esta forma se trata de evitar que las estaciones transmitan simultáneamente. Si lo hacen, entonces se busca que sea de forma controlada. También se intenta tratar de serializar el envío de datos al poner a dormir al transmisor. La cantidad de éxitos aumenta a un 37%. Acá no se puede realizar detección de portadora.

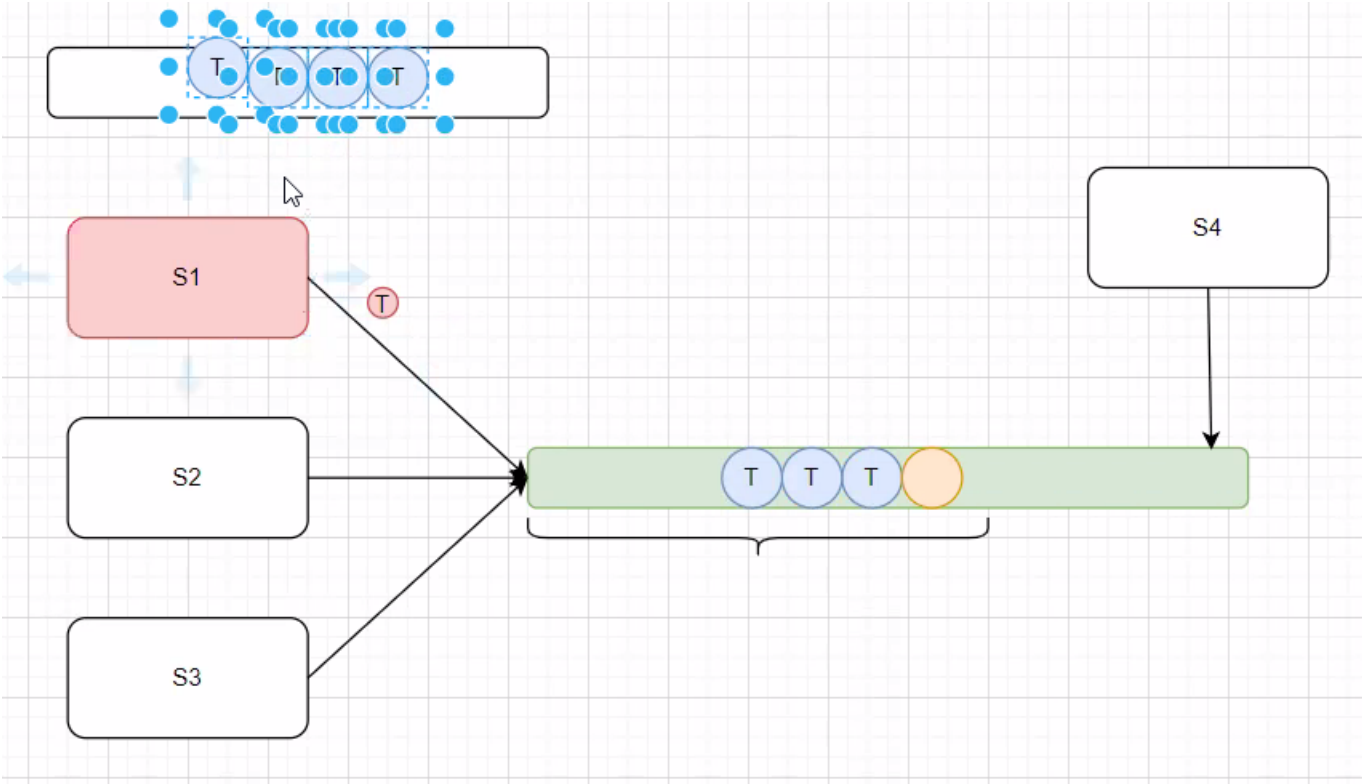
Uso de portadoras

La portadora dice que una entidad de transporte puede ir y verificar el medio. Cuando verifica el medio se puede dar cuenta si alguien está transmitiendo. Si alguien lo está haciendo, entonces se duerme un rato

esperando a que el medio se desocupe. En una estación inalámbrica como medio esto es prácticamente imposible.



En el medio de cobre, se debe esperar un cierto tiempo al enviar una trama para asegurarse que una estación se adueñó del medio. Las estaciones pueden hacer una detección temprana de colisión. Envían una trama y esta vuelve, posiblemente con menor potencia. Si hay otra trama, entonces esta al volver volverá distinta, entonces se sabe que hay otra trama. El proceso en el que la estación se queda escuchando se conoce como feedback. Se queda escuchando hasta que recibe lo que escuchó, para saber que el canal está libre.



Las transmisiones al ser en ráfagas, lo suyo sería canalizar el envío de tramas, colocando la mayor cantidad posible de tramas por el canal para que se muevan juntas. No obstante, si se enviaron algunas tramas y se detectó que chocaron, entonces el canal detiene la transmisión y no va a enviar el resto de tramas hasta que

el canal esté desocupado. Al despertarse intenta detectar portadora, si no está presente entonces intenta enviar otra vez y así sucesivamente.

Ethernet Clásica

Ethernet Clásica (IEEE 802.3)

- Ya no se usa.
- Velocidades 3 a 10 Mbps.
- Un sólo cable alrededor de un edificio, dónde se conectan las computadoras.
- Ethernet gruesa: Cable amarillo grueso con marcas cada 2.5 mts para conectar las computadoras.
  - 500 mts por segmento
- Ethernet delgada: Mas fácil de doblar e implementar.
  - 185 mts por segmento
- Ocupa repetidores
- Datos codificados en Manchester
- Usa CSMA/CD con retroceso exponencial binario

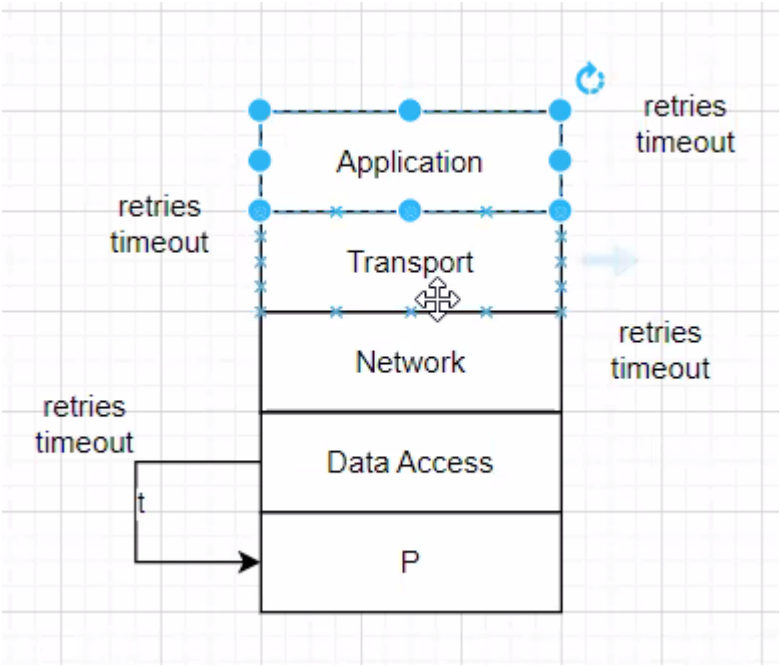
Cable muy grande que cada 2.5m se conectaba a un equipo. Para conectar varios sementos se ocupaba un repetidor o bridge.

Ethernet Conmutada

Ethernet Conmutada (802.3)

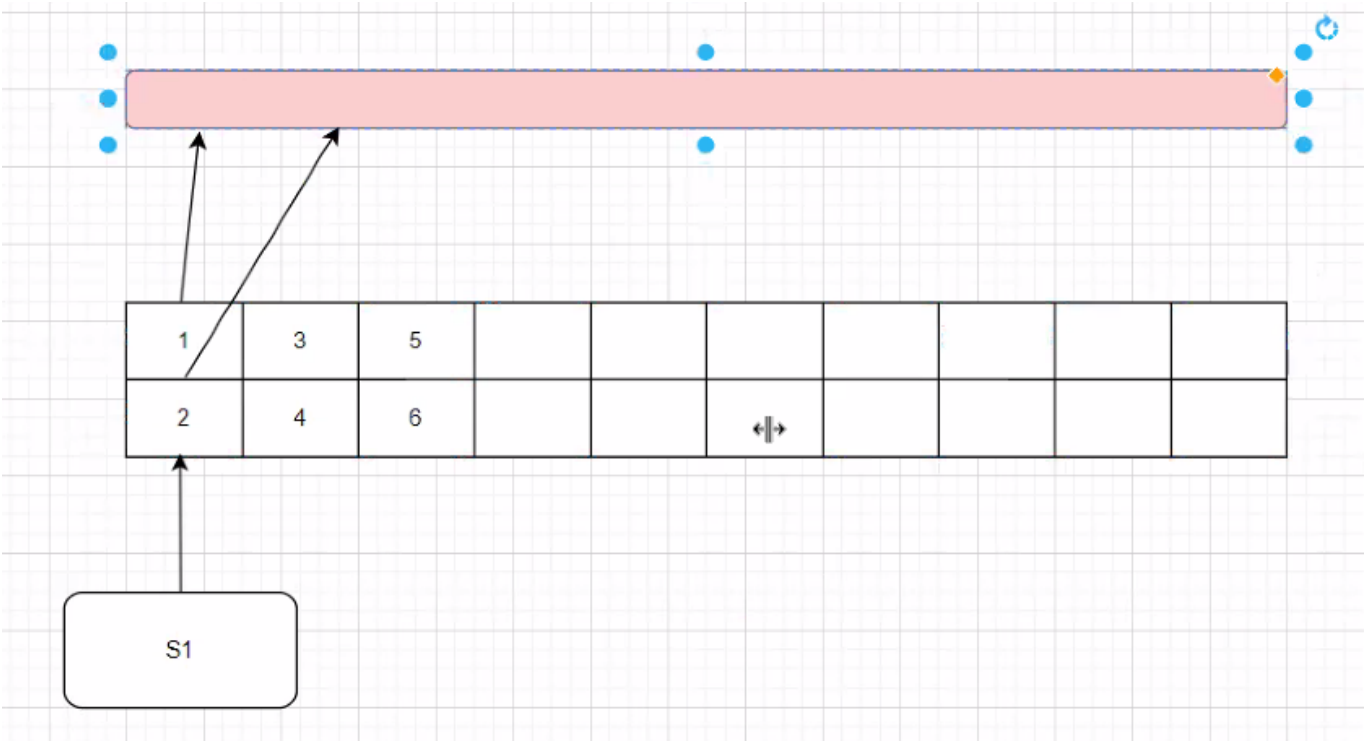
- Fast Ethernet (100 Mbps), Gigabit Ethernet (1Gbps) y 10 Gigabit Ethernet (10Gbps). Autonegociación
- Cada estación cuenta con un cable (par trenzado de teléfono) dedicado que llega al **hub** central.
  - Un hub conecta todos los cables que llegan a él.
  - Los hubs conectan todas las estaciones y los paquetes se entregan por difusión.
  - Todas las estaciones están en el mismo dominio de colisión (existen colisiones)
- El hub fue cambiado por un switch:
  - El switch sabe que estaciones están conectadas en sus puertos
  - Sólo envía los paquetes a las estaciones destino (modo promiscuo)
  - Cada estación es su dominio de colisión.
    - Si es full duplex, no existen colisiones.
    - Si es half duplex, se participa por el canal con las tramas que entran al switch y salen del switch.
  - Se pueden enviar múltiples tramas.
  - Dispositivo caro
  - Mejora el rendimiento.
  - Tiene buffers

Mucho más rápida. La difusión es un desperdicio del ancho de banda ya que se envían paquetes a todas las estaciones de la red, sin importar si a estos no les interesa recibirlo.



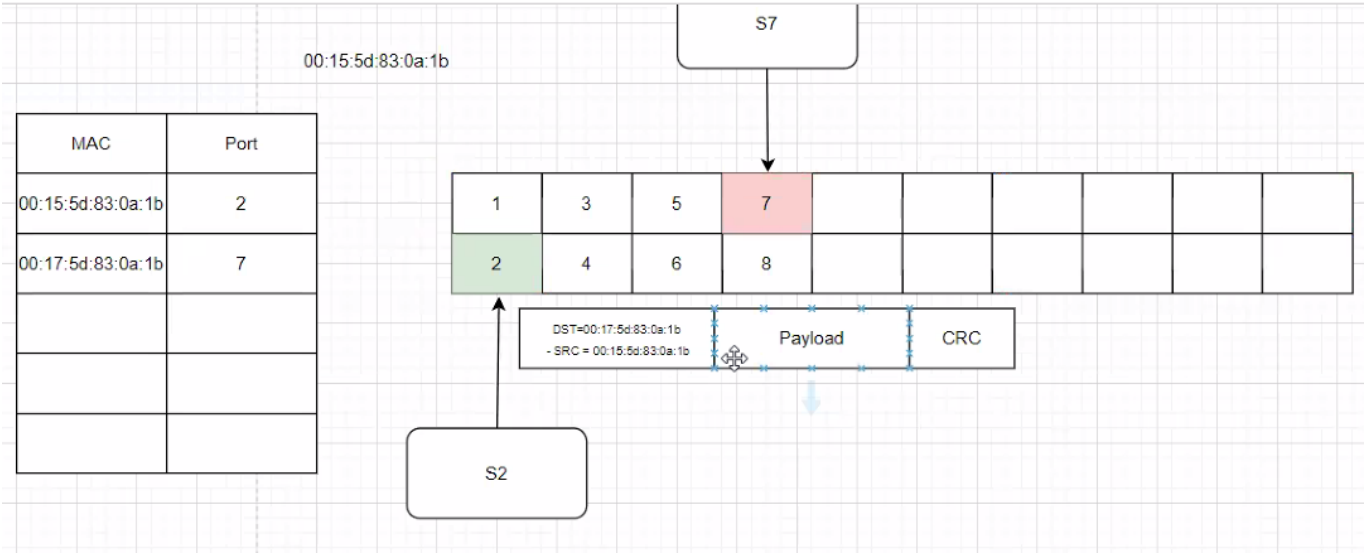
Cuando en una capa de acaban los retries, se le pasa el problema a la siguiente capa y así sucesivamente hasta que se llega a la capa de aplicación y se acaban los retries. Entonces ahí se da un error de conexión.

Adelanto sobre Hubs



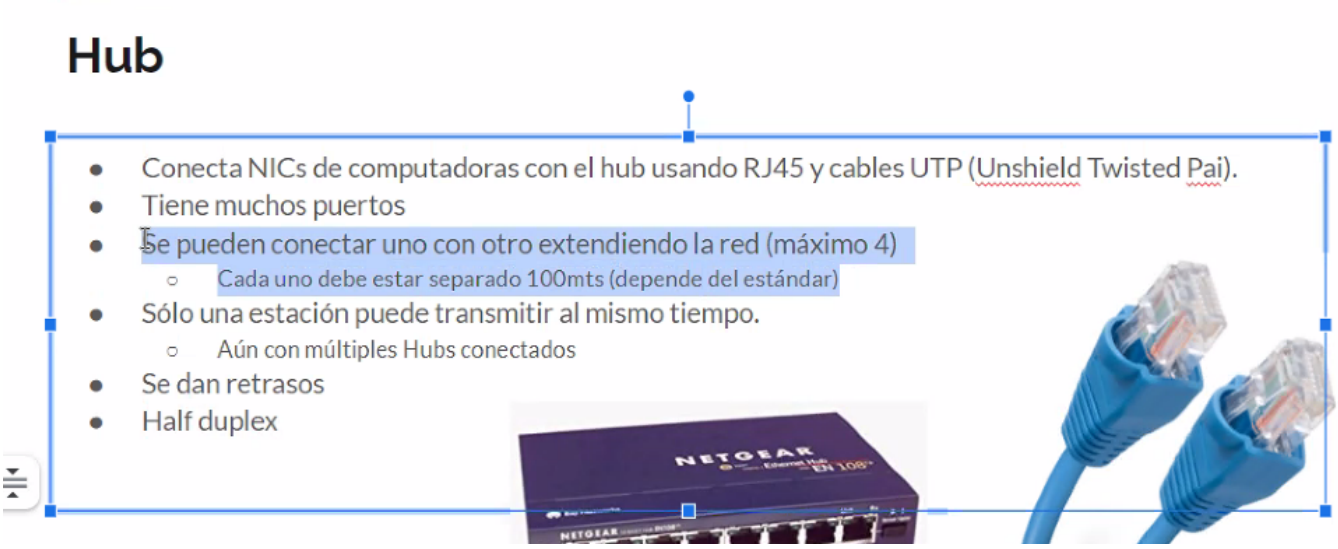
En un hub se tiene un único bus de transmisión y se pueden conectar muchos dispositivos a los puertos. La probabilidiad de colisión es muy alta. El switch da como ventaja, por un precio más alto.

Adelanto sobre Switches



Si en un switch se conecta a un puerto una estación, entonces la estación dice aquí estoy mediante el MAC address. El switch tiene una tabla que tendrá una relación entre MAC address y la estación., además de otra información. Cuando la segunda computadora se conecta a otro puerto, indica su MAC address. Cuando el paquete sale de la estación, en el DST (Destination) va el MAC address del destinatario y en el SRC (Source) el de quien lo envía. Entonces el switch genera una conexión llamada circuito virtual entre el puerto emisor y receptor de la información. Este circuito virtual es punto a punto, por lo que es como tener un cable única y exclusivamente para esos puertos. Entonces el vector de colisión pasa de tener muchos puertos a solo 2.

Conmutación de la capa de enlace de datos



Lo subrayado corresponde a la forma de hacer que funcionen como solo una red. No se deben conectar más de cuatro hubs porque si no se empiezan a experimentar más problemas de red.

Repetidores

Repetidores

- Regeneran la señal.
- Amplificación de señal.
- Proporciona extender el rango de una LAN.
- Permite dar potencia a la señal para que puede viajar mas distancia.
- Puede conectar dos o mas segmentos (hubs)
- Permite el desarrollo de PoE
  - Power over Ethernet

Implican un aumento de la señal. Si se conectan varios repetidores juntos, no se podrá reconocer la señal, lo que equivale a perder los datos.

Bridges

Bridge

- Conecta dos segmentos de red.
- Puede incluir las funcionalidades de un repetidor.
- Filtra el tráfico que se mueve entre dos LAN.
- Define políticas de seguridad separando diferentes grupos viviendo en las redes.
- Transparente para las estaciones.

Permite conectar dos segmentos de red. Las tablas de los switches entonces se vuelven tablas globales. Cualquier dispositivo puede establecer un circuito virtual con otro dispositivo conectado al switch. El bridge permite implementar políticas de seguridad y controlar el tráfico. También permite implementar un repetidor. A nivel de bridge se puede limitar el acceso a un switch en específico.

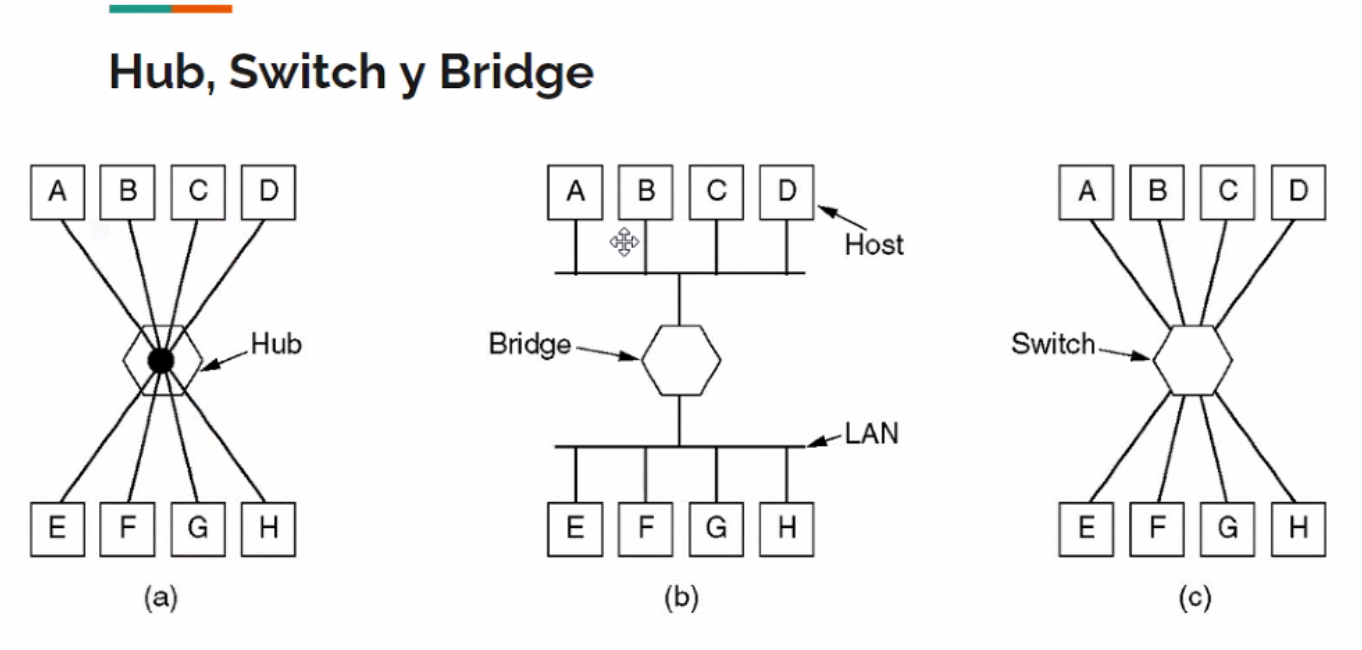
Switches

Switches

- Similar a un bridge
- Permite conectar muchísimos segmentos.
- Permite realizar múltiples configuraciones.
  - Virtual LANs (VLAN)
- Es inteligente para entregar las tramas a las estaciones adecuadas.
  - Reduce el gasto de ancho de banda.
- Seguridad: Sólo ven los paquetes que se les envían, a menos que este en modo promiscuo.
- Full duplex
- Caros comparados con hubs
- No existe límite de switches interconectados.

En los hubs, al tener un dominio de colisión muy solo, entonces si uno fuera un usuario malicioso que coloca una estación para robar toda la transmisión de una red, entonces se conecta a un puerto y no envía datos, solo captura todo lo que llega. Una estación, al enviar un paquete al dominio de colisión, este es recibido por todas las máquinas conectadas al dominio de colisión. Esto porque todas deben realizar detección de portadora, al ser un medio compartido. En un hub no hay mucha seguridad. Por otra parte, en un switch, hay mucha seguridad ya que se generan estos circuitos virtuales y se hacen conexiones 1 a 1, por lo que no hay oportunidad de robar los datos. Todo esto de Ethernet conmutada aplica para un medio de transmisión cableado. En el momento que se entra a Wireless, todo esto no aplica.

Hub, Switch y Bridge



De esta forma se ven los vectores de colisión de los hub, switches y bridges.

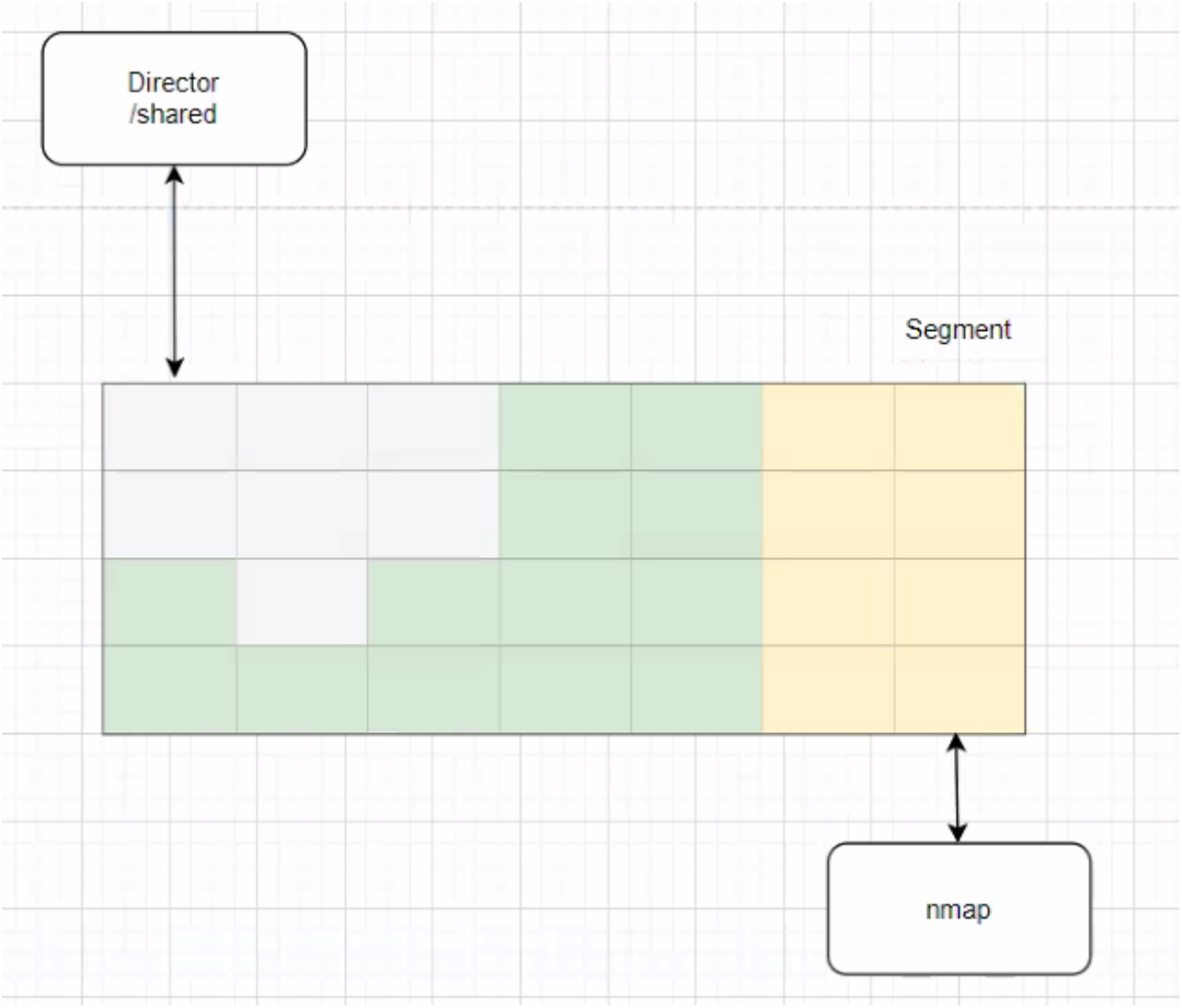
Virtual LAN

Virtual LAN

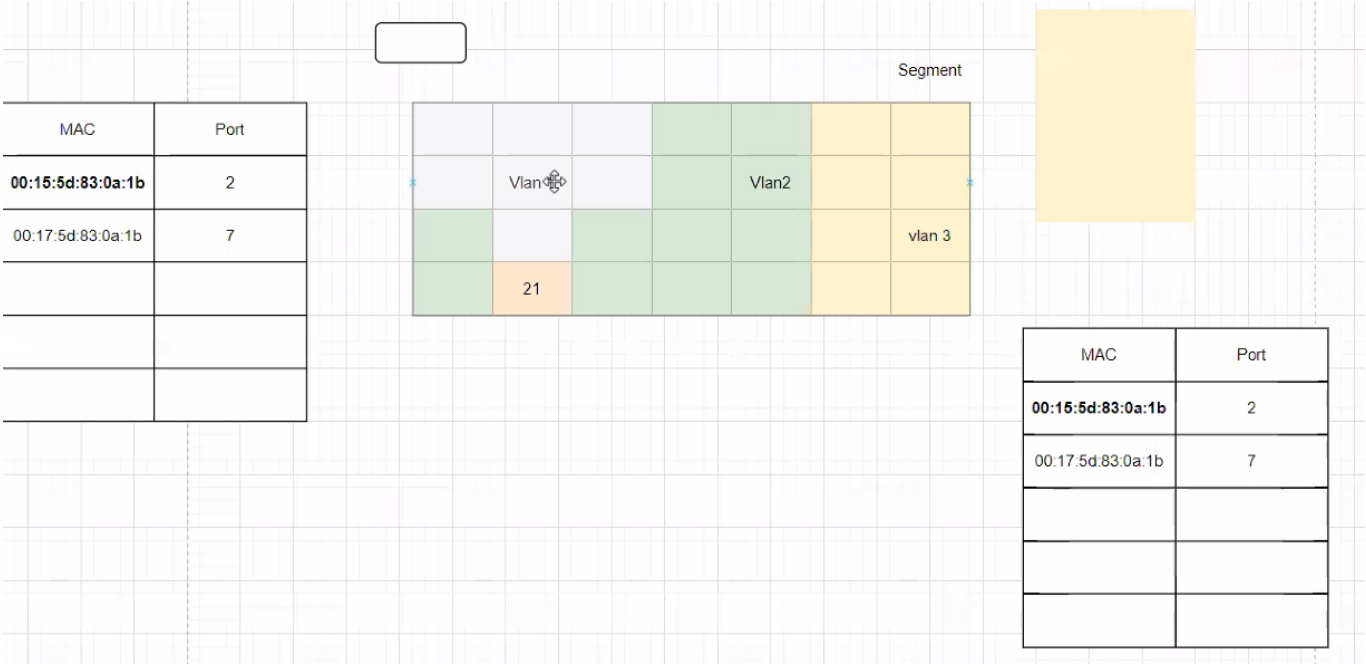
- Se pueden comprar varios switche para crear LAN separadas.
- Organizar usuarios en redes para reflejar la estructura de la organización.
- Unas LAN se usan mas que otras, evitar saturación.
- Difusión: No se envían paquetes no deseados.
- Switches diseñados con está capacidad.
- Se decide en cuantas VLAN se divide un switch
    - Asigna un número
    - Cada VLAN se le asigna una cantidad de puertos.

Cuando se tiene un switch, físicamente dicho switch es un solo segmento de red. Esto lo que quiere decir es que va a tener una tabla que permitirá direccionar y establecer circuitos virtuales entre diferentes máquinas conectadas en una red. Suponga entonces que una computadora se pegó al switch y por mala configuración se dejó un directorio compartido con información sensible. Luego llega otra computadora que se conecta al mismo switch. Si en esta otra computadora se ejecuta un nmap, entonces se puede obtener el ip de la primera máquina, lo que permite obtener el MAC address. Entonces se puede establecer una conexión de la máquina 2 a la 1. Esto ocurre ya que un switch físicamente es un segmento de red, pero uno normalmente no deja puertos para un uso específico en un mismo segmento.

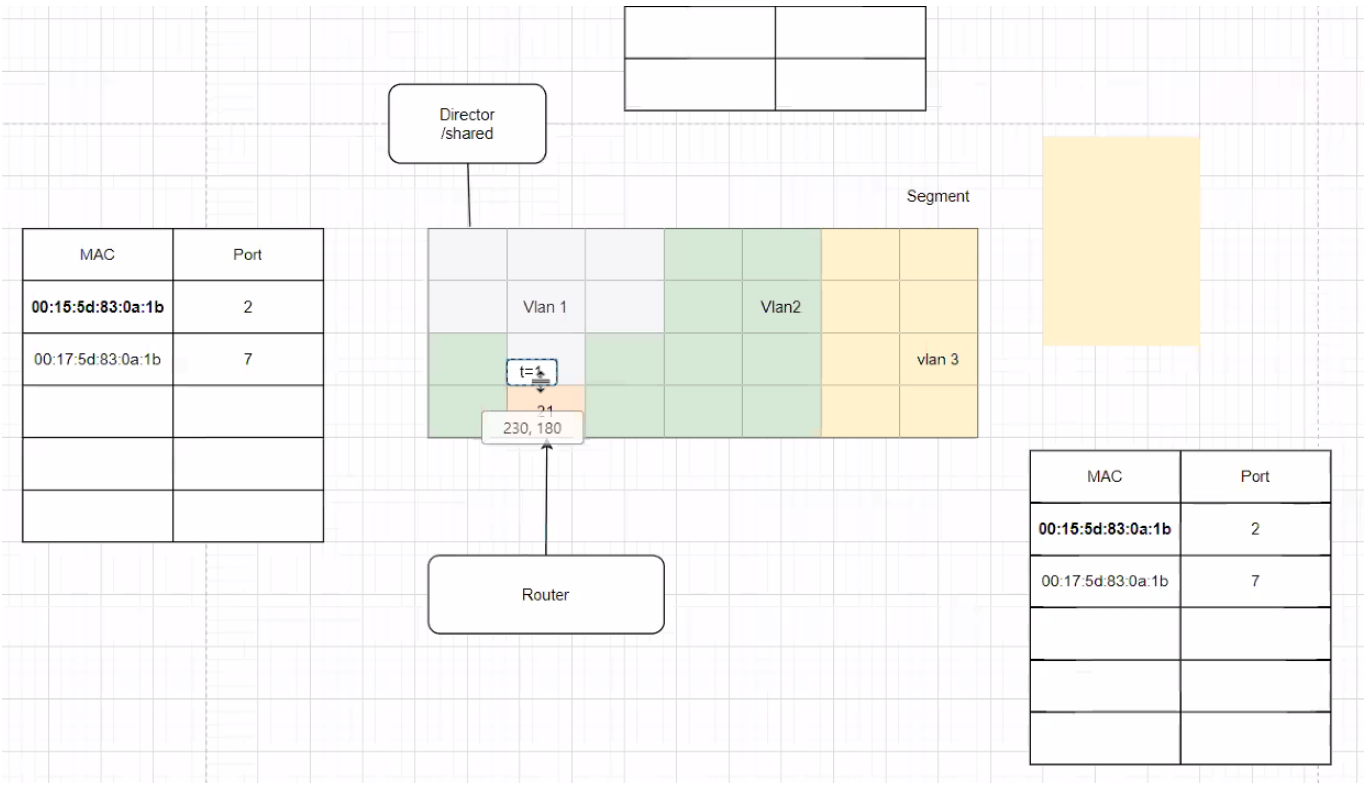
Segmentación de una VLAN



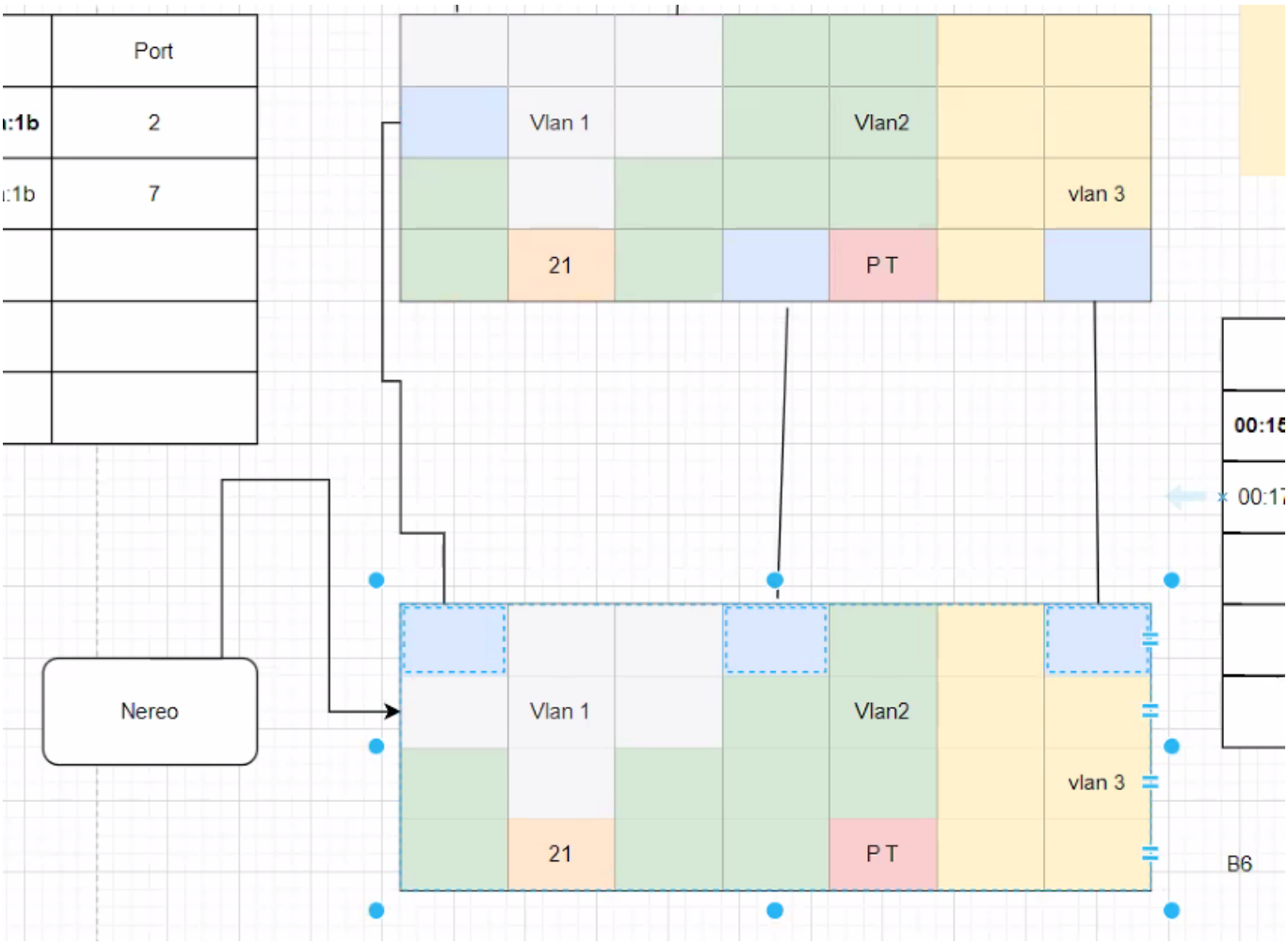
En un punto, surgió la necesidad de tener segmentos lógicos. Se toma un grupo de puertos y se convierten en un segmento lógico. Esto garantiza que el switch tendrá tablas para cada uno de los segmentos. Esto implica que, aunque la primera computadora tenga una carpeta compartida con información sensible, al ejecutar nmap desde la segunda máquina y se averigue la ip de la primera máquina, no hay forma de acceder. Al tener VLANs, entonces cada segmento lógico es como si se tuviera un propio switch físico.



Una VLAN permite hacer más cosas. También se puede tomar un puerto y definirlo como un trunk o puerto troncal. Esto significa que este puerto pertenece a las VLANs que se le indique. Esto implica que todas las tramas que viajan dentro de los segmentos llevarán un tag. A cada VLAN se le da un número. Entonces al definir el puerto trunk, al definir una máquina que se pegue al puerto trunk, dicha máquina tiene acceso a las 3 VLAN del ejemplo. Entonces se le debe poner un tag a la trama para saber a donde debe ir.



Cuando la máquina 1 envía una trama a internet, cuando esta pasa por el puerto 21, entonces se le coloca el tag a la trama. Cuando se recibe la trama devuelta, entonces el switch sabe a quién le debe entregar el paquete por la trama. Otra cosa que se puede realizar es definir un puerto en modo promiscuo. Un puerto de un segmento de red se va a comportar como un hub. Si se pega una estación en un puerto en modo promiscuo, se logra pegar un dispositivo de red y se empieza a capturar todo el tráfico hacia capas superiores en un segmento lógico de red. También se puede definir simultáneamente en modo trunk. Entonces esto permite poder comerse todo el tráfico de la red. Esto se usa con protocolos como Netflow para realizar análisis del tráfico en la red.



Otra configuración que se puede hacer es acceder a recursos de una VLAN desde otra. Entonces se puede extender el segmento tirando un cable desde un puerto del segmento por ejemplo de administrativos a otro puerto de la red de administrativos. Esto tiene un gran desperdicio ya que son puertos inutilizados para comunicar los switches. Con más VLANs se desperdician más puertos. Entonces lo que se puede hacer es desperdiciar solo 2 puertos. Estos puertos serían configurados como troncales, lo que haría unir los segmentos de red. No tienen necesariamente que ser los mismos puertos o segmentos. Lo único importante es que los segmentos lógicos tengan el mismo número de VLAN, luego se definen los puertos trunk e inmediatamente las redes se unirán de forma lógica. De esta forma se pueden tener más switches conectados físicamente para ampliar los segmentos lógicos.