Crypo-Tag Switching
And
Flow Paths

Flow Based Routing

- Data plane packets can be crypto tag switched through the core network (between replicators)
- Packets are forwarded using a reactive flow based routing mechanism
- Reactive routing determines the “path” from origin to destination on demand as a reaction to the need to forward
- We call that path a “flow”. Each flow is stored in a flow table, managed by the replicators
- When a new “flow” is needed, meaning a new flow from an origin device to a destination device is needed, then the replicator asks the MCP what replicator it should forward the traffic through.
- If the destination device is attached to a replicator, then the MCP informs the first replicator as to which replicator it should forward the traffic through. This process of reactively creating a flow is only done once at the beginning of a session through the core. After that, an entry is created in each replicator involved in the flow to define what the next hop should be.
- As each subsequent packet arrives at the origin replicator, then the flow table tells that replicator what the next hop is. The packet can then be forwarded directly to the destination replicator without consulting the MCP.
- As packets arrive at a destination replicator a check is made to see if a “reverse flow” exists for the path from the destination device back to the origin device. If not, a flow entry is created at the destination replicator to facilitate routing back through the reverse path.
- The flow tables allow replicators to manage fault conditions effortlessly — for example when either the origin or destination device becomes disconnected or even if one of the replicators goes off line.

Flow Table

Flow ID	Flow
127	Flow ID Origin Endpoint ID Destination Endpoint ID Next Hop Endpoint ID
***	***

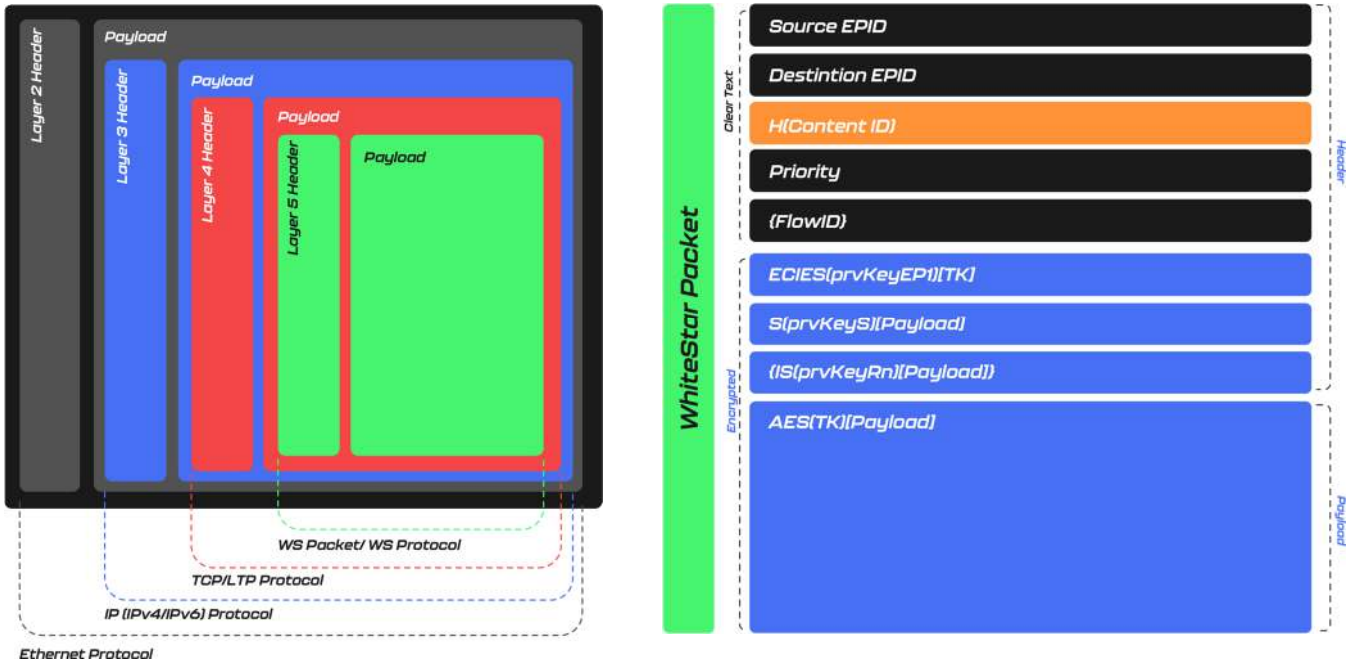
Crypto Tag Switching

- Crypto Tag Switching allows the WhiteStar NOS to cryptographically forward only trusted packets from an origin device to a destination device while at the same time making it impossible for the replicators to actually decrypt the packet. This is a patented WhiteStar technology.
- Here's how it works: image that we have two devices and two replicators. One of the devices is the origin device and the other is the destination device. The origin device is attached to an origin replicator and the destination device is connected to a destination replicator. The two replicators are also connected to each other.
- By connected, we mean that they have a peer to peer session established between cohort pairs. So three sessions:
  - From the origin device to the origin replicator.
  - From the original replicator to the destination replicator.
  - From the destination replicator to the destination device
- This chain of cohort pairs allows us to form an end to end trust chain, without the intermediate nodes (replicators) needing to decrypt the packets as the flow through them.
  - Origin device trusts origin replicator. Origin replicator trusts origin device.
  - Origin replicator trusts destination replicator. Destination replicator trusts origin replicator.
  - Destination replicator trust destination device. Destination device trusts destination replicator.
  - And finally origin device trusts destination device and destination device trusts origin device.

Crypto Tag Switching - Trust Chains

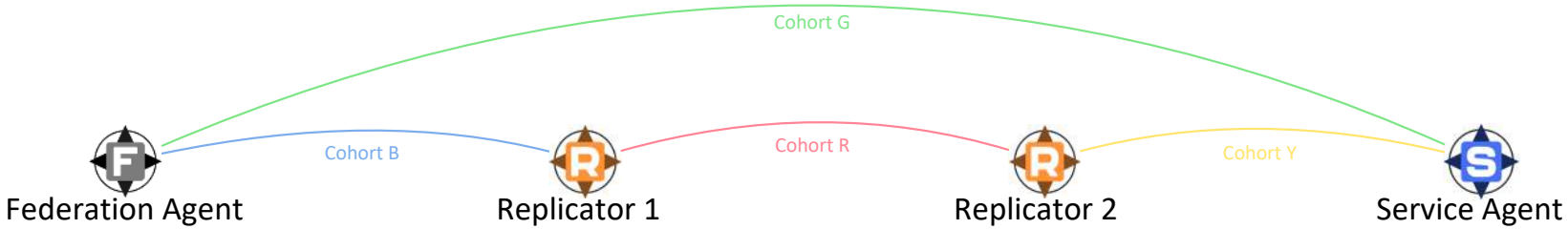
- Now the origin device wants to send a packet to the destination device:
  - First, the origin device generates a new temporal key and derives a new public/private key pair for the packet.
  - The origin device them encrypts the temporal key with the destination devices newly derived public key.
  - Then the origin device encrypts the payload with the temporal key and signs the packet with its private key.
  - The origin device then sends the packet to the original replicator. The origin replicator notes that the destination is some other device, checks for a flow ID and resolves it if not found. It then checks the origin device's signature to make sure its not a replay or DOS attack. The origin replicator can do this because it has a trust relationship with the origin device. On the other hand the origin replicator can't decrypt the packet because it does not have the destination devices key chain.
  - Assuming the packet is good, the origin device then "signs" the packet with an intermediate signature using its private key. It forwards the packet to the destination replicator.
  - When the destination replicator get the packet, it sees that its for the destination device. It checks and amends its flow table. It sees that it came form the origin replicator. It checks and removes the intermediate signature. It can do this because it has a trust relationship with the origin replicator. Again the destination replicator can extend the trust chain, but can't decrypt the packet because it does not have the destination device's private key chain. The packet is then forward to the destination device.
  - The destination device sees that the packet is from the origin device. It checks the signature to make sure it was really from the origin. It checks the origin device's signature to make sure that the packet has not been altered. It them generates its next private key and decrypts the temporal key. Using the temporal key it then decrypts the payload.

Anatomy of a WhiteStar Packet



- The source and destination addresses of the packet are Endpoint IDs
- A content tracking ID can be optionally attached to the packet
- Each packet has end to end priority which is enforced at each node of the WhiteStar Network
- If the packet is crypto tag switched, then a flow ID is used to securely manage the flow of packets
- Each packet contains a encrypted temporal key (TK), secured by a unique public/private key pair which changes on each packet
- Each packet contains a signature of the entire packet using the source's private key
- If the packet is crypto tag switched, then it also includes an intermediate signature created using the previous hop's private key
- The payload is then encrypted with the temporal key (TK) using a quantum-resistant symmetric encryption algorithm
- Only the destination endpoint can decrypt the packet

Crypto Tag Switching - Data Plane



Four cohorts are shown, each in a different color to illustrate that each pair are using unique encryption chains. What this means is that a packet, encrypted by the *federation agent* to be sent to the *service agent* (using the green cohort G) can only be decrypted by the *service agent* and no other element.

Ideally, all the elements shown can form "peer to peer" connections with each other (see black lines below.) Most of the time they will. However, there are times when a cohort pair can't form a peer to peer connection and therefore they need some way to communicate with each other, even without the peer to peer connection. This is what crypto tag switch provides.