

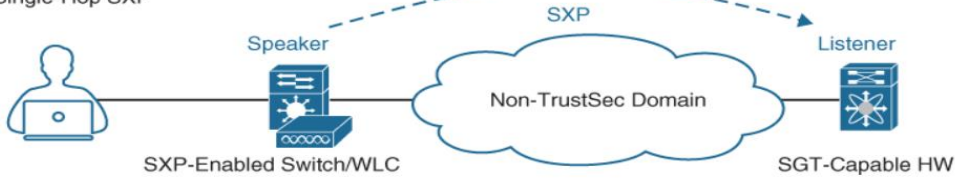
TrustSec:

- o TrustSec is next-generation access control enforcement solution developed by Cisco.
- o To address the growing operational challenges related to maintaining firewall rules.
- o To maintaining the Firewall rules and ACLs by using Security Group Tag (SGT) tags.
- o It uses SGT tags perform ingress tagging & egress filtering enforce access control policy.
- o Cisco ISE assigns the SGT tags to users or devices that are successfully authenticated.
- o Cisco ISE assigns the SGT tags to users authorized through 802.1x, MAB, or WebAuth.
- o The SGT tag assignment is delivered to the authenticator as an authorization option.
- o After SGT tag is assigned, an access enforcement policy allow or drop based on SGT tag.
- o After SGT tag is assigned SGT Tag can be applied at any egress point of TrustSec network.
- o The SGT tags represent the context of the user, device, use case, or the function.
- o This means SGT tags are often named after particular roles or business use cases.
- o The SGT name is available on Cisco ISE and the network devices to create policies.
- o What is actually inserted into a Layer 2 frame SGT tag is basically a numeric value.
- o It Config occurs three phases Ingress classification, Propagation & Egress enforcement.

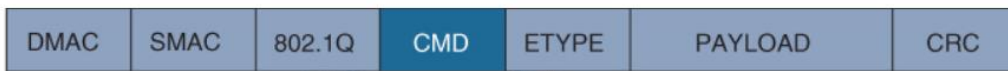
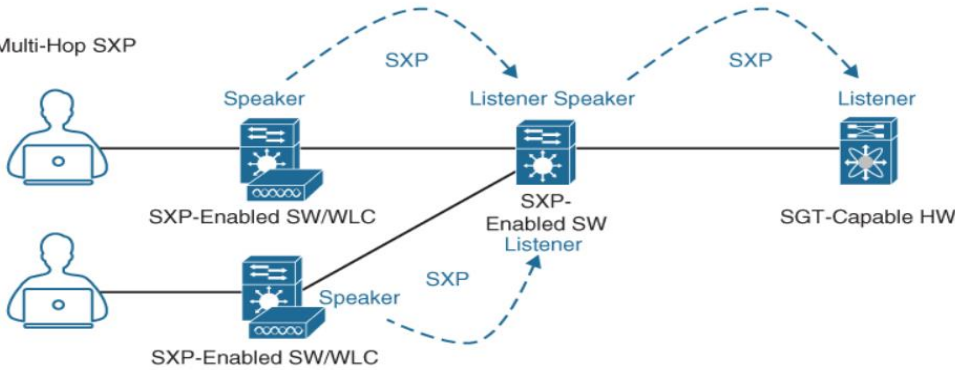
| Icon | Name | SGT (Dec / Hex) | Description |
|------|---------------------|-----------------|------------------------------------|
| | Auditors | 9/0009 | Auditor Security Group |
| | BYOD | 15/000F | BYOD Security Group |
| | Contractors | 5/0005 | Contractor Security Group |
| | Developers | 8/0008 | Developer Security Group |
| | Development_Servers | 12/000C | Development Servers Security Group |
| | Employees | 4/0004 | Employee Security Group |
| | Guests | 6/0006 | Guest Security Group |

| Source | BYOD (15/000F) | Contractors (5/0005) | Development_Servers (12/000C) | Employees (4/0004) |
|-------------------------------|----------------|----------------------|-------------------------------|--------------------|
| Auditors (9/0009) | Deny IP | Deny IP | Deny IP | Deny IP |
| BYOD (15/000F) | Permit IP | Deny IP | Deny IP | Deny IP |
| Contractors (5/0005) | Deny IP | Permit IP | Deny IP | Deny IP |
| Developers (8/0008) | Deny IP | Deny IP | Permit IP | Deny IP |
| Development_Servers (12/000C) | Deny IP | Deny IP | Deny IP | Deny IP |
| Employees (4/0004) | Deny IP | Deny IP | Deny IP | Permit FTP |

Single-Hop SXP

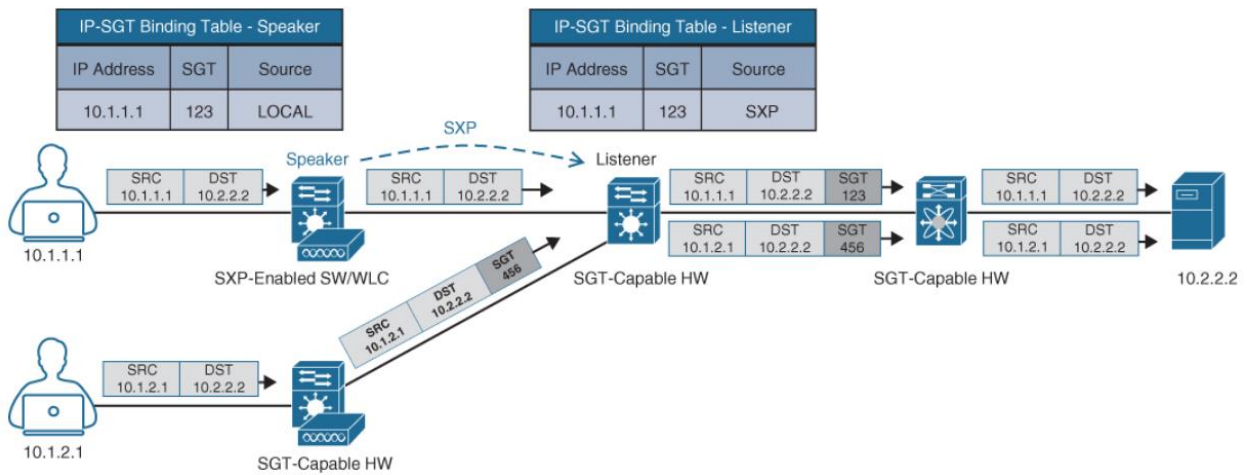


Multi-Hop SXP



Cisco Metadata

16-Bit (64K Name Space)



MACsec:

- o MACsec is an IEEE 802.1AE standards-based Layer 2 hop-by-hop encryption method.
- o In MACsec the traffic is encrypted only on the wire between two MACsec peers.
- o In MACsec the traffic is unencrypted as it is processed internally within the switch.
- o This allows the Cisco switch to look into the inner packets for things like SGT tags.
- o To perform packet enforcement or Quality of Service (QoS) etc prioritization.
- o MACsec also leverages onboard ASICs to perform the encryption and decryption.
- o Rather than having to offload to a crypto engine, as with Internet Protocol Security.
- o It is based on Ethernet frame format; an additional 16-byte MACsec Security Tag field.
- o MACsec provides authentication using Galois Method Authentication Code (GMAC).
- o Authenticated encryption using Galois/Counter Mode Advanced Encryption Standard.

