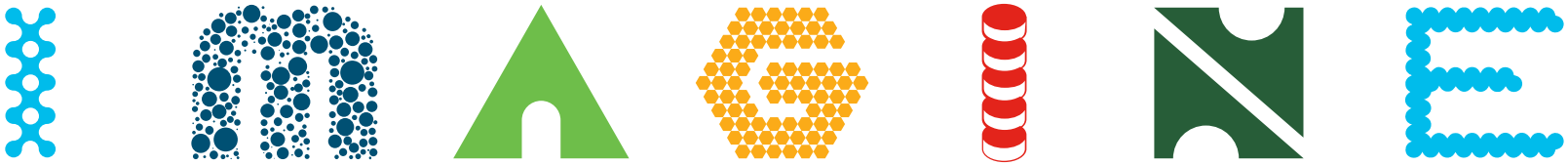


INTUITIVE

Cisco live!

June 10-14, 2018 • Orlando, FL

#CLUS

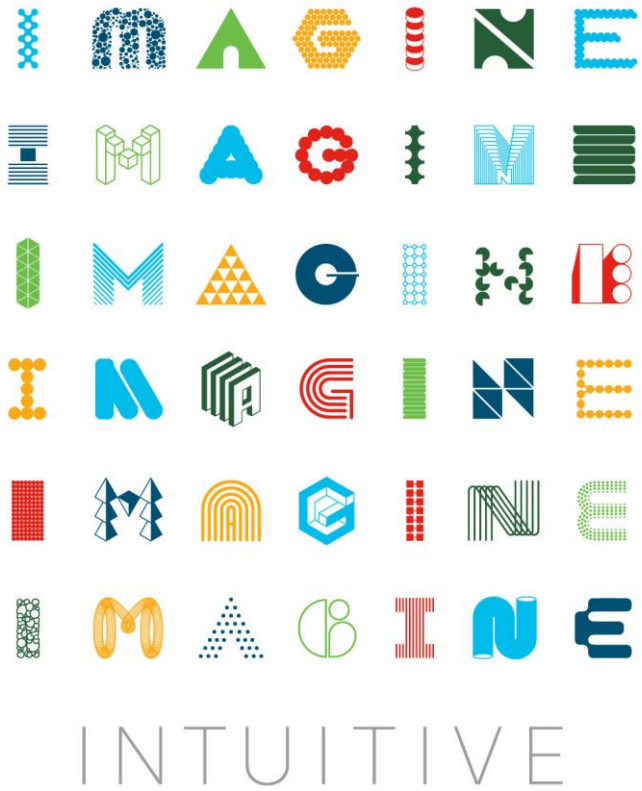
Introduction to WAN MACsec

Aligning Encryption Technologies with WAN Transport

Craig Hill – Distinguished SE (@netwrkr95)

Stephen Orr – Distinguished SE (@StephenMOrr)

BRKRST-2309



Agenda

- Introduction
- Transport Types
- MACSec overview
- MACSec Key Agreement (MKA)
- WAN MACSec Deployment Models
- High Availability
- APIs/Programmability
- Conclusion

Cisco Webex Teams

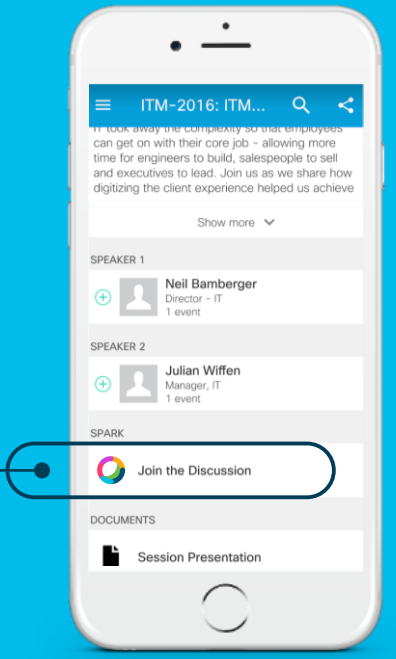
Questions?

Use Cisco Webex Teams (formerly Cisco Spark) to chat with the speaker after the session

How

1. Find this session in the Cisco Events App
2. Click “Join the Discussion”
3. Install Webex Teams or go directly to the team space
4. Enter messages/questions in the team space

Webex Teams will be moderated by the speaker until June 18, 2018.



cs.co/ciscolivebot#BRKRST-2309

Session Presenters

Craig Hill

Distinguished System Engineer

US Public Sector

CCIE #1628

Stephen Orr

Distinguished System Engineer

US Public Sector

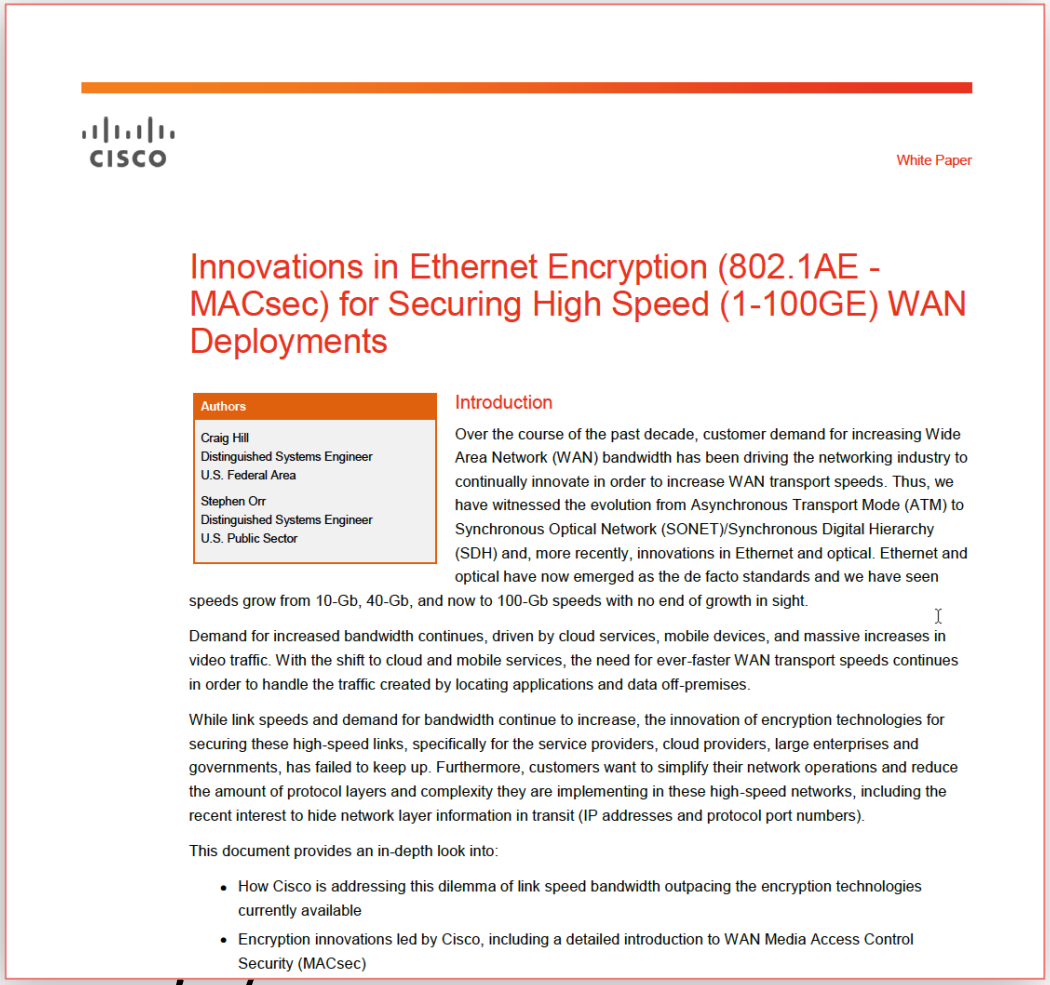
CCIE #12126

What we hope to Achieve in this session:

- Understanding that data transfer requirements are exceeding what IPSec can deliver
- Introduce you to new encryption options evolving that will offer alternative solutions to meet application demands
- Enable you to understand what is available, when and how to position what solution
- Understand the right tool in the tool bag to meet encryption requirements
- Understand the pros/cons and key drivers for positioning an encryption solution
- What key capabilities drive the selection of an encryption technology

Session Assumptions and Disclaimers

- Intermediate understanding of Cisco Site-to-Site Encryption Technologies
  - DMVPN
  - GETVPN
  - FlexVPN
- Intermediate understanding of Ethernet, VLANs, 802.1Q tagging
- Intermediate understanding of WAN design, IP routing topologies, peering vs. overlay
- Basic understanding of optical transport and impact of OSI model on various layers (L0 – L3) of network designs
- Many 2 hour breakout sessions will focus strictly on areas this presentation touches on briefly (we will provide references to those sessions)



White Paper

Innovations in Ethernet Encryption (802.1AE - MACsec) for Securing High Speed (1-100GE) WAN Deployments

Authors

Craig Hill
Distinguished Systems Engineer
U.S. Federal Area

Stephen Orr
Distinguished Systems Engineer
U.S. Public Sector

Introduction

Over the course of the past decade, customer demand for increasing Wide Area Network (WAN) bandwidth has been driving the networking industry to continually innovate in order to increase WAN transport speeds. Thus, we have witnessed the evolution from Asynchronous Transport Mode (ATM) to Synchronous Optical Network (SONET)/Synchronous Digital Hierarchy (SDH) and, more recently, innovations in Ethernet and optical. Ethernet and optical have now emerged as the de facto standards and we have seen speeds grow from 10-Gb, 40-Gb, and now to 100-Gb speeds with no end of growth in sight.

Demand for increased bandwidth continues, driven by cloud services, mobile devices, and massive increases in video traffic. With the shift to cloud and mobile services, the need for ever-faster WAN transport speeds continues in order to handle the traffic created by locating applications and data off-premises.

While link speeds and demand for bandwidth continue to increase, the innovation of encryption technologies for securing these high-speed links, specifically for the service providers, cloud providers, large enterprises and governments, has failed to keep up. Furthermore, customers want to simplify their network operations and reduce the amount of protocol layers and complexity they are implementing in these high-speed networks, including the recent interest to hide network layer information in transit (IP addresses and protocol port numbers).

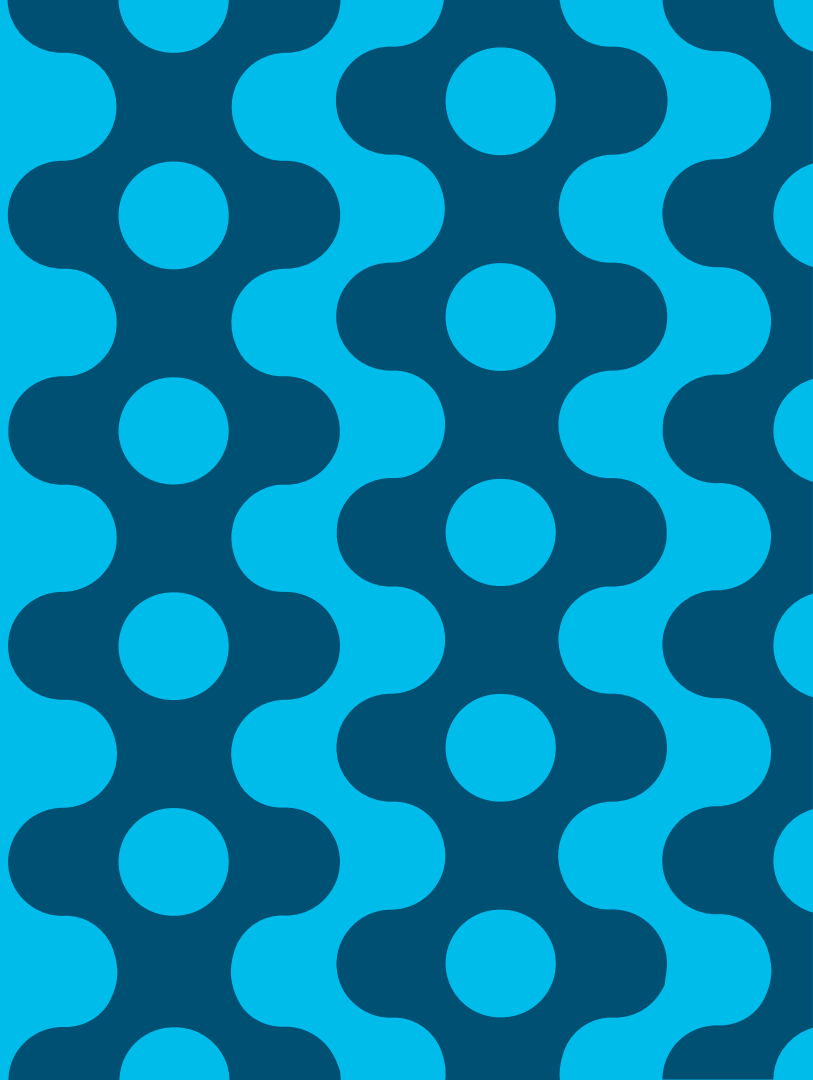
This document provides an in-depth look into:

- How Cisco is addressing this dilemma of link speed bandwidth outpacing the encryption technologies currently available
- Encryption innovations led by Cisco, including a detailed introduction to WAN Media Access Control Security (MACsec)

Public Link:

http://www.cisco.com/c/dam/en/us/td/docs/solutions/Enterprise/Security/MACsec/WP-High-Speed-WAN-Encrypt-MACsec.pdf

Cisco’s Next Generation Encryption Initiative



Cisco live!

Cryptography

The Universal Security Feature

Crytography is embedded in all of Cisco's products

Cryptography is critical to every solution and market

Vital to Cybersecurity efforts within all of our customers

Where Cryptography is Deployed Today

Authentication

- TLS based Protocols
  - EAP-TLS
  - PEAP
  - EAP-FAST
- Hashing
  - SHA1
  - SHA256/384/512
- Digital Signatures
- Key Negotiation

Privacy/Confidentiality

- IPSec
- SRTP
- DTLS
- SSL
- 802.1AE (MACSec)
- 802.11i (802.11-2012)
- RADSec

Management

- SSH
  - sFTP
  - SCP
- HTTPS
- FTPs

What is Next Generation Encryption (NGE)?

Cryptographic Technologies

- New/Upgraded algorithms, key sizes, protocols and entropy
- Compatible with existing security architectures

Secure and Efficient

- Algorithm efficiency enabling increased security
- Scales well to high/low throughput

Compatible with Government Standards

- CNSA(US)
- FIPS-140 (US/Canada)
- NATO

Next Generation Encryption: Why it's Needed...

- Next Generation Encryption (NGE)
  - A widely accepted and consistent set of cryptographic algorithms that provide strong security and good performance
  - Best standards that can be implemented today to meet the security and scalability requirements for network security in the years to come
  - No attacks against these algorithms have been demonstrated.

- Quantum Computing – a different paradigm in computing
  - A quantum computer could break public key cryptography standards in use today.
  - While no practical quantum computer is known to be available today, the risk does exist.
  - Information with long-term confidentiality requirements should be protected against future decryption (i.e., capture now, decrypt when quantum computers become viable.)
    - Data-in-transit (e.g., capture data communications)
    - Data-at-rest (e.g., capture file images)

Cryptography Recommendations

Operation	Algorithm		
	Acceptable	NGE (preferred)	QCR
Encryption	AES-CBC mode	—	✓ (256-bit)
Authenticated encryption	—	AES-GCM mode	✓ (256-bit)
Integrity	—	SHA-256 / 384 / 512	✓ (384/512)
Integrity	HMAC-SHA-1	HMAC-SHA-256	✓ (256-bit key)
RSA: Key exchange / Encryption / Authentication	DH / RSA / DSA -2048 / 3072 / 4096	ECDHE / ECDSA-384 / 521	
ECC: Key exchange / Authentication	ECDHE / ECDSA-256	ECDHE / ECDSA-384 / 521	

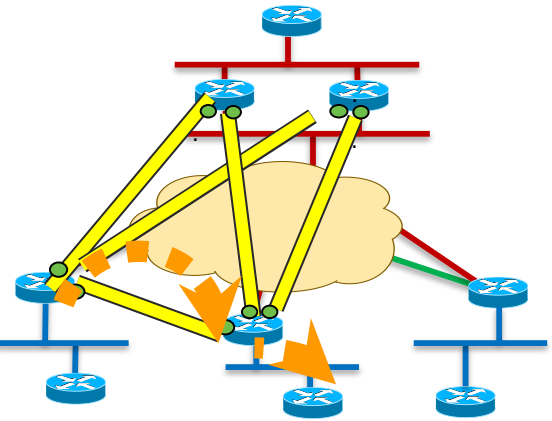
QCR = quantum computer resistant.

Recommended algorithms per security level

Algorithm		Security level (strength)
Acceptable	NGE	
AES-128-CBC DH, DSA, RSA-3072 - HMAC-SHA-1	AES-128-GCM ECDHE, ECDSA-256 SHA-256 HMAC-SHA-256	128 bits
AES-192-CBC - - -	AES-192-GCM ECDHE, ECDSA-384 SHA-384 HMAC-SHA-256	192 bits
AES-256-CBC - - -	AES-256-GCM ECDHE, ECDSA-521 SHA-512 HMAC-SHA-256	256 bits

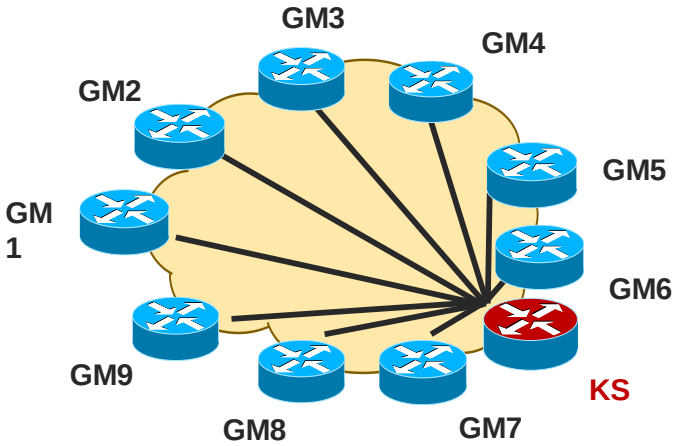
Customers concerned with QC Resistance should use NGE recommended algorithms (>128-bit security level)

NGE Enabled Encryption Architectures: Available Today

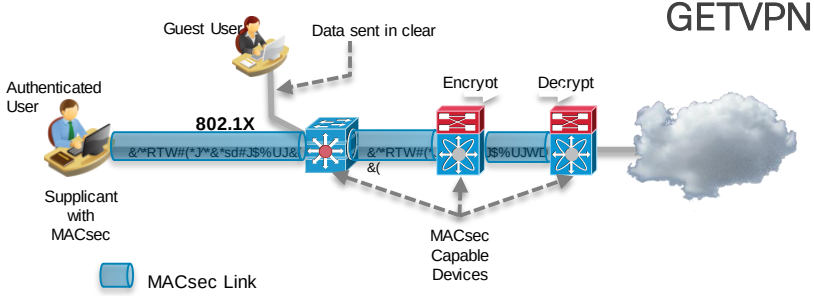


Site to Site, DMVPN, and FlexVPN

Remote Access VPNs



GETVPN



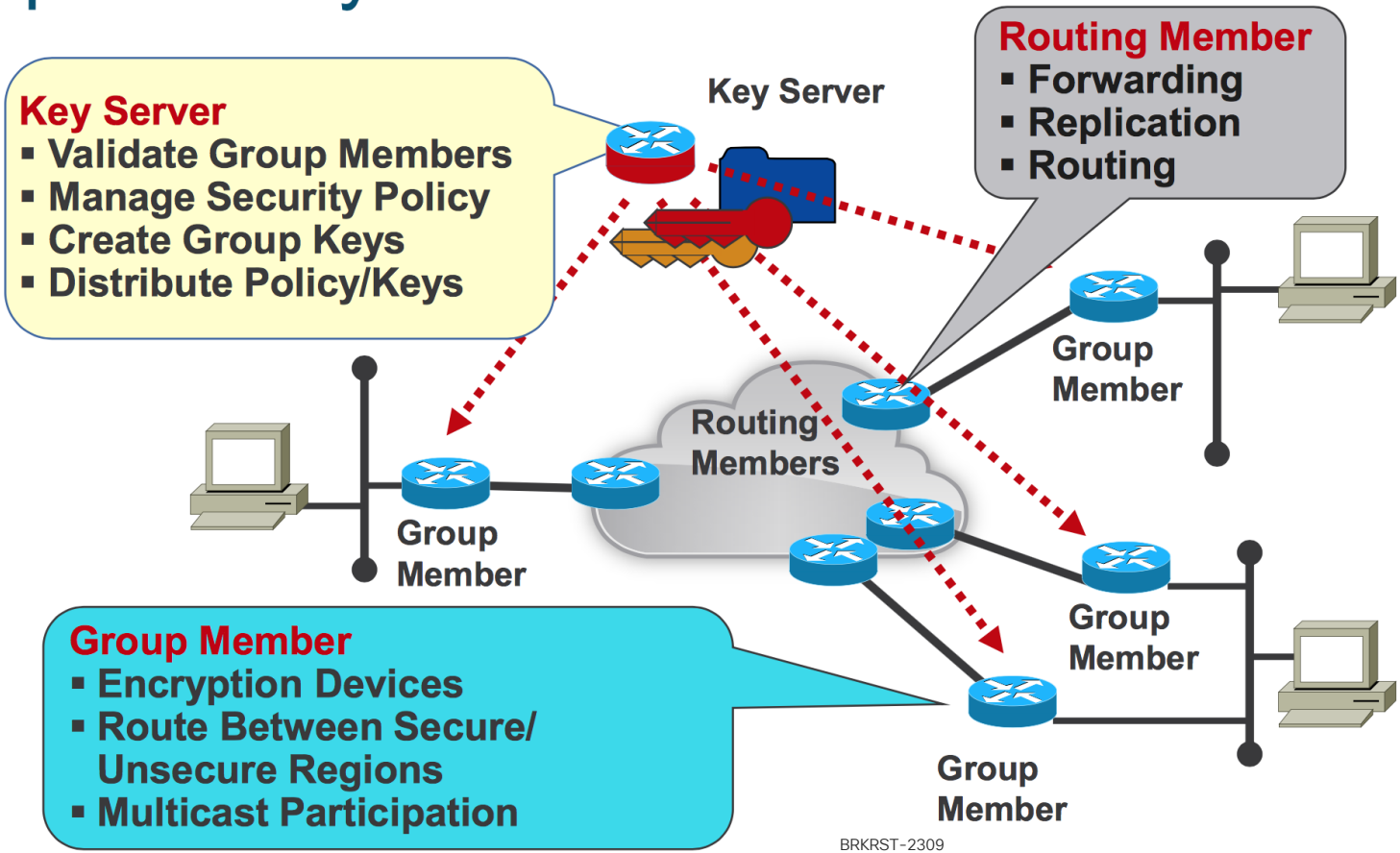
MACsec

VPN Solutions Compared

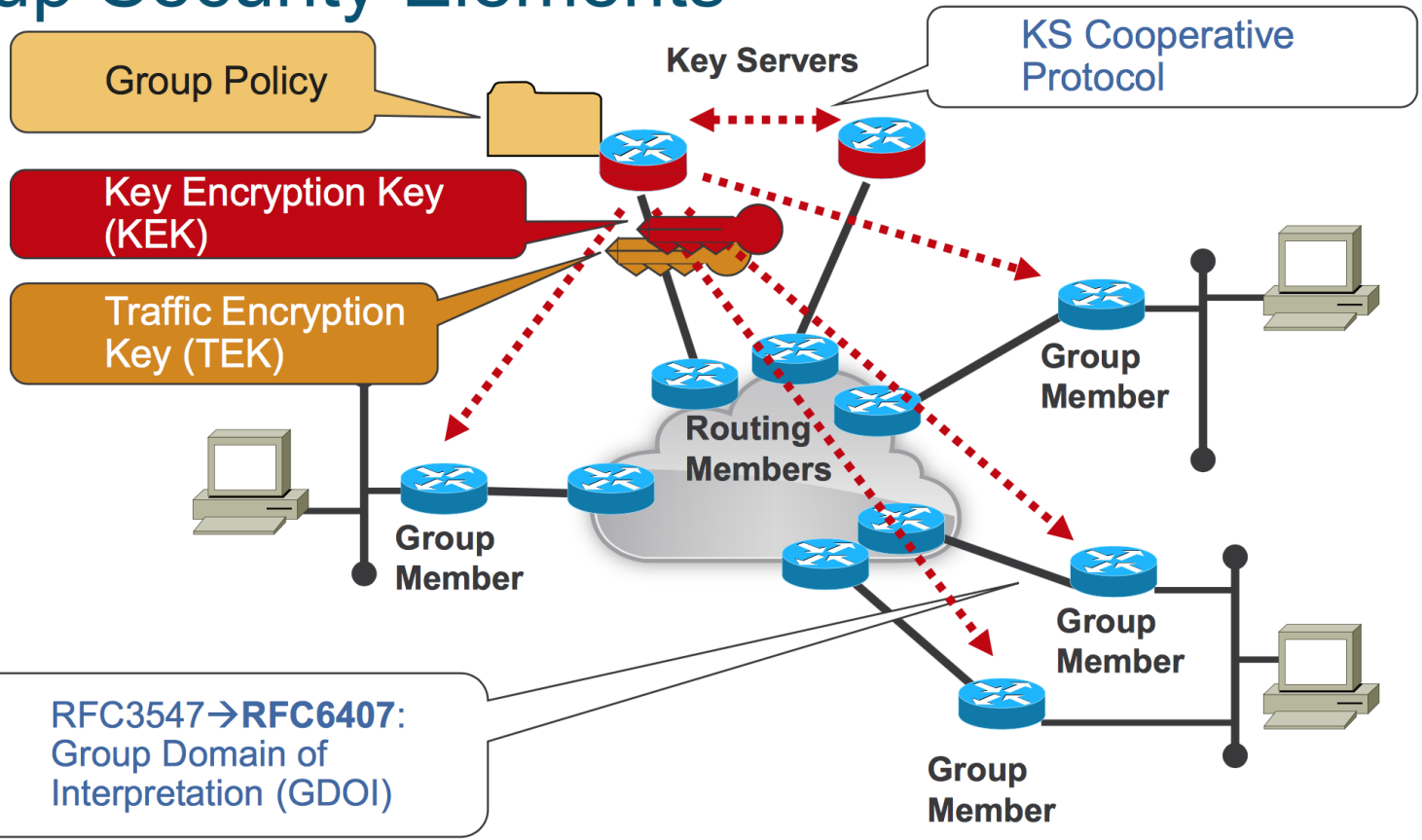
	DMVPN	FlexVPN	GET VPN
Network Style	▪ Large Scale Hub and Spoke with dynamic Any-to-Any ▪ Up to 4000 sites	▪ Converged Site to Site and Remote Access ▪ Up to 10000 sites	▪ Any-to-Any; (Site-to-Site) ▪ 24,000 group members per KS
Failover Redundancy	▪ A/A based on Dynamic Routing	▪ Dyn Routing or IKEv2 Route Distribution ▪ Server Clustering ▪ Stateful Failover *	▪ Transport Routing ▪ COOP Based on GDOI
IP Multicast	▪ Multicast replication at hub	▪ Multicast replication at hub ▪ Multicast replication in IP WAN network *	▪ Multicast replication in IP WAN network
QoS	▪ Per Tunnel QoS, Hub to Spoke	▪ Per SA QoS, Hub to Spoke ▪ Per SA QoS, Spoke to Spoke*	▪ Transport QoS
Policy Control	▪ Locally Managed	▪ Centralized Policy Management	▪ Locally Managed
Technology	▪ Tunneled VPN ▪ Multi-Point GRE Tunnel ▪ IKEv1 or IKEv2	▪ Tunneled VPN ▪ Point to Point Tunnels ▪ IKEv2 Only	▪ Tunnel-less VPN ▪ Group Protection
Infrastructure Network	▪ Public or Private Transport ▪ Overlay Routing	▪ Public or Private Transport ▪ Overlay Routing	▪ Private IP Transport ▪ Flat/Non-Overlay IP Routing
3rd Party Compatibility	▪ No	▪ Yes – up to 3rd party implementation	▪ No

GETVPN

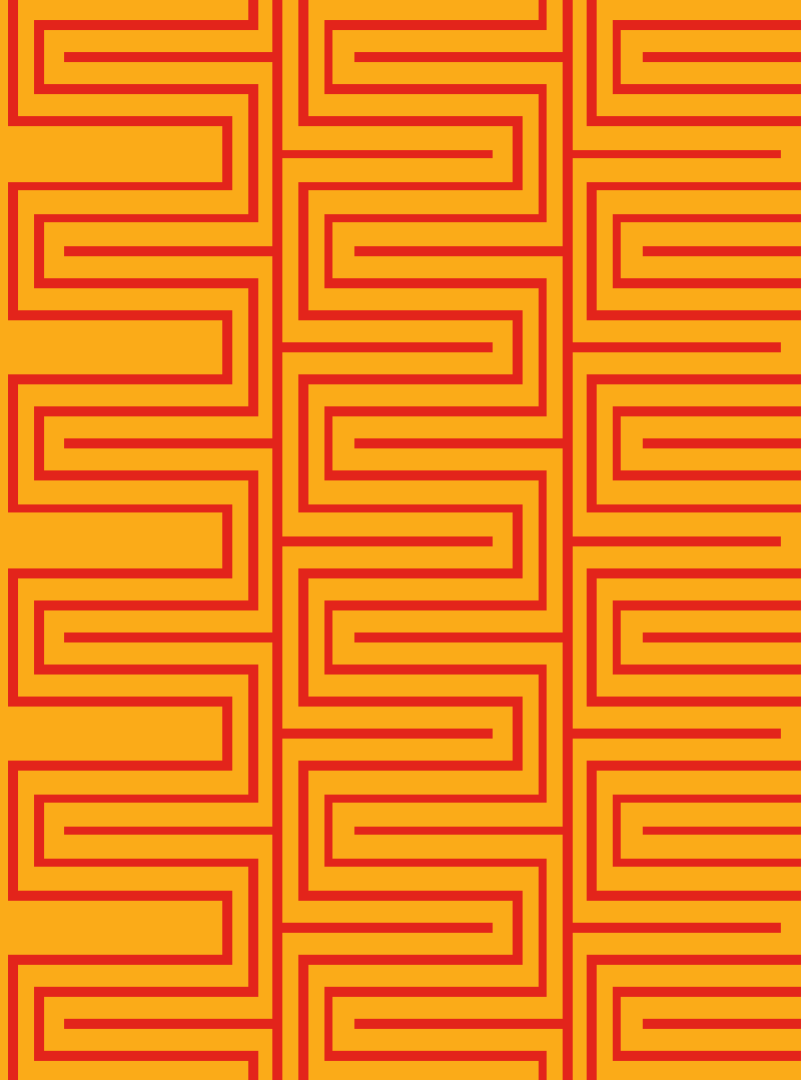
Group Security Functions



Group Security Elements



Evolving Encryption Solutions – Introduction to MACsec

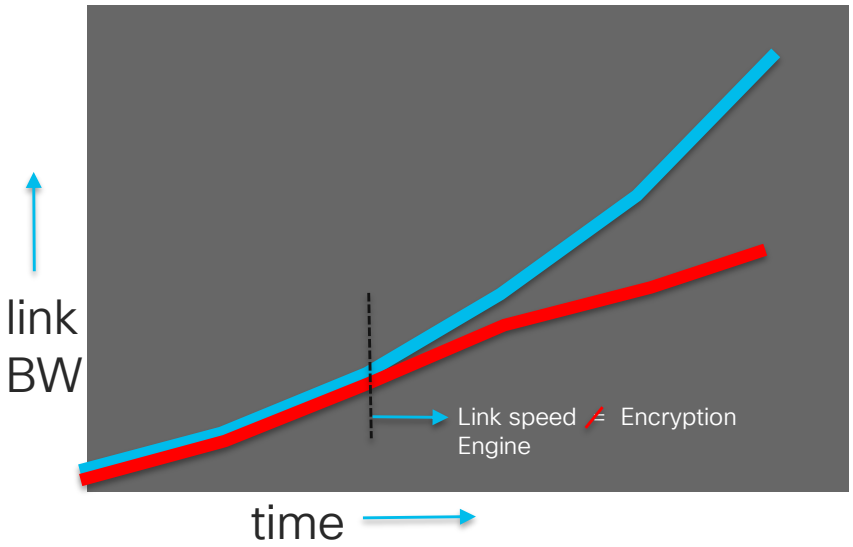


Challenges with Current WAN Encryption

- IPSec performance, complexity, and cost becoming more challenged
  - Throughput constrained to the performance of the IPSec encryption engine
- MPLS, Multicast, IPv6 in some cases require GRE tunneling to operate
  - GRE and IP overlays add an additional leverage of complexity and performance impact in certain router platforms
- Innovations such as DMVPN, MPLS VPN over mGRE simplify this, but IPSec performance still lowest common denominator and performance impact
- Line-rate encryption is becoming a requirement, that is simpler to operate, and removes levels of complexity from the WAN solution

WAN MACsec targets addressing these challenges…

Link Speeds Out-Pacing IP Encryption



- Bandwidth application requirements out-pacing IP encryption capabilities
- Bi-directional and packet sizes further impact encryption performance
- IPSec engines dictate aggregate performance of the platform (much less that router forwarding capabilities)
- Encryption must align with link speed (100G+) to support next-generation applications

Problems addressed by L2 Encryption

- IPSec performance, complexity, and cost becoming more challenged
- Performance at a fraction of overall router throughput
- High-speed solutions target line-rate encryption
- Solves Architectural complexity
- Removes packet size/MTU issues
- Obscures IP and MPLS content

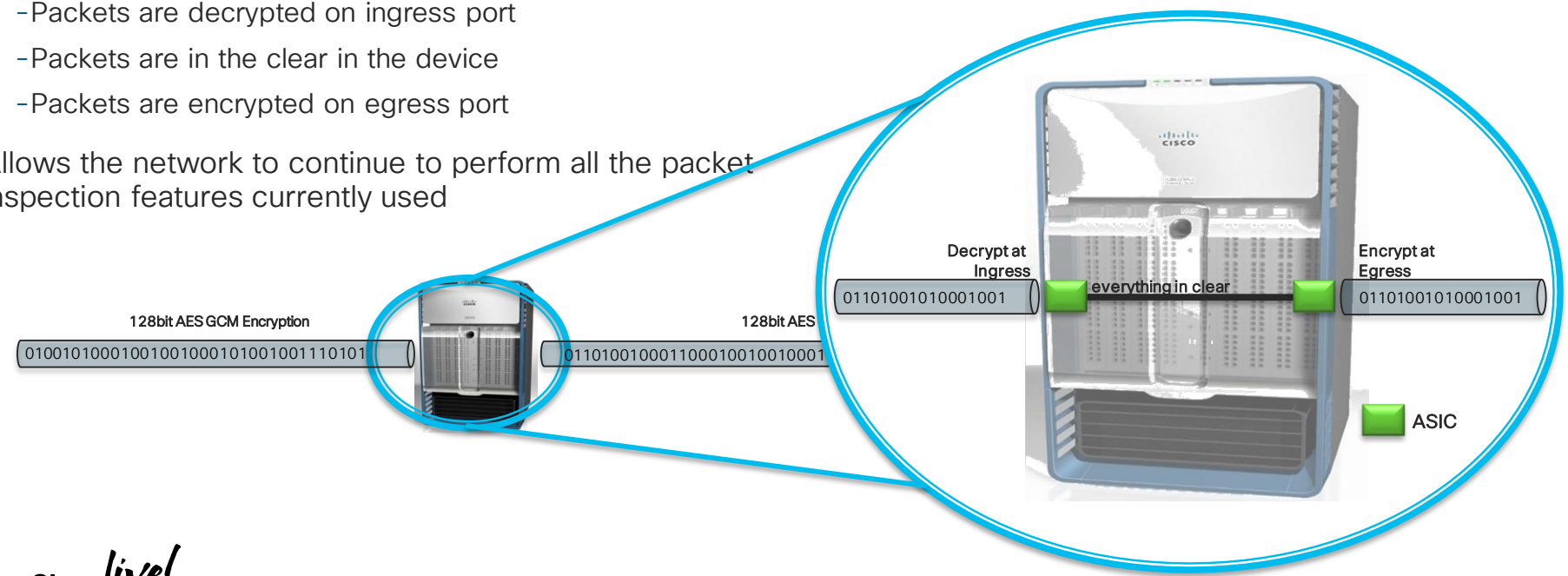
OTN and WAN MACsec targets these challenges…

New Applications and Architectures Driving WAN Encryption Rates

- Increasing bandwidth demands over the WAN for branch, applications and data centers
- Less applications run locally in branch locations, driving high-speed transport increases
- Highly resilient cloud computing architectures (C2S, GovCloud) driving high speed data center replication requirements
- Traffic pattern changes dictated by cloud, M2M communications, IoT/IoE
- Encryption landscape is changing driving high speed layered encryption solution offerings

What is MAC Security (MACsec)? Hop-by-Hop Encryption via IEEE802.1AE

- Hop-by-Hop vs End-to-End "Bump-in-the-wire" model
  - Packets are decrypted on ingress port
  - Packets are in the clear in the device
  - Packets are encrypted on egress port
- Allows the network to continue to perform all the packet inspection features currently used



Confidentiality and Integrity 802.1AE based Encryption

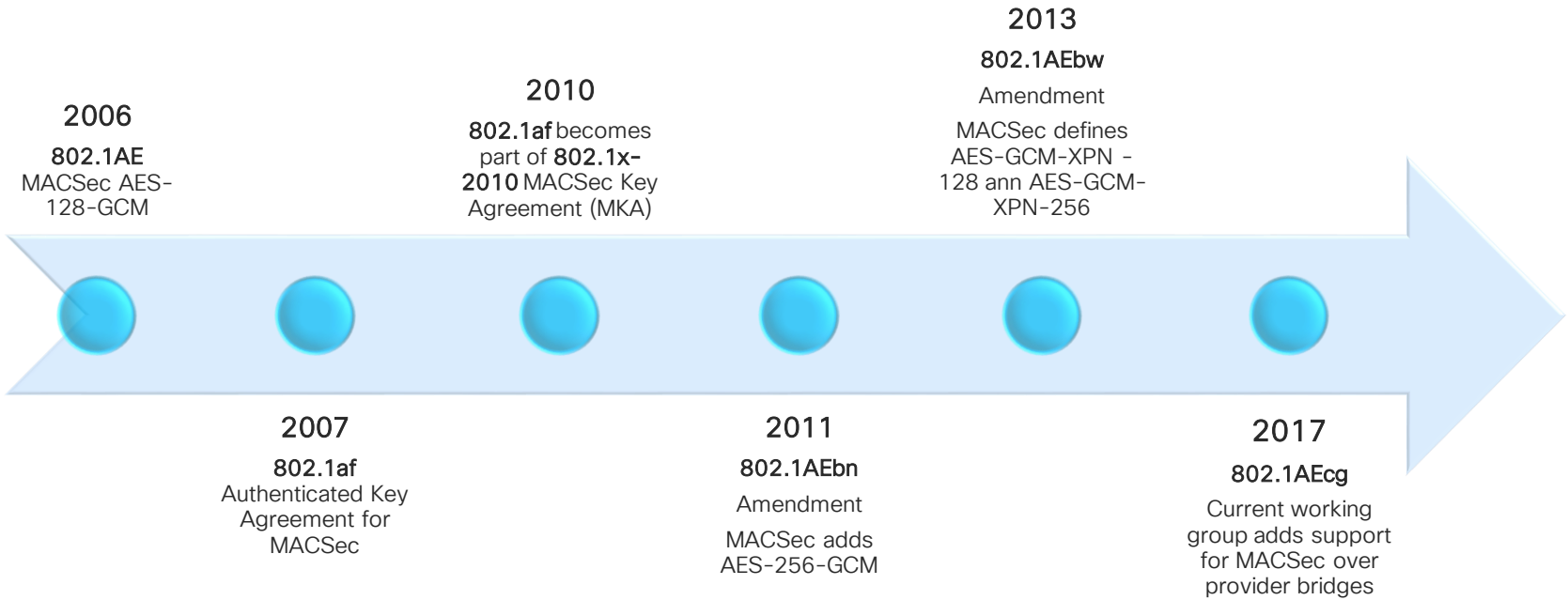
- * NIST Special Publication 800-38D (http://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf)

- MACsec provides Layer 2 hop-by-hop encryption and integrity, based on IEEE 802.1AE standard
- 128/256 bit AES-GCM (Galois/Counter Mode) – NIST Approved *
- Line rate Encryption / Decryption for both 1/10/40/100GbE interface
- Replay Protection of each and every frame

Customer Benefits

- Protects against man-in-the-middle attacks (snooping, tampering, replay)
- Standards based frame format and algorithm (AES-GCM)
- 802.1X-2010/MKA addition supports per-device security associations in shared media environments (e.g. PC vs. IP Phone) to provide secured communication
- Network service amenable hop-by-hop approach compared to end-to-end approach (e.g. Microsoft Domain Isolation/virtualization)

MACsec Timeline

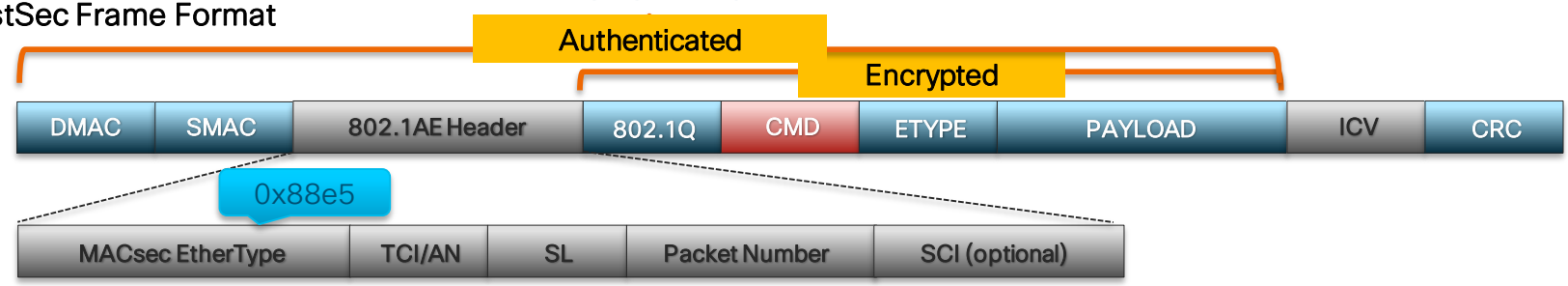


MACsec Protocols & Algorithms

	Function	Protocol	Specification	Encryption Algorithms
1	Device Identification	Secure Device Identification	IEEE 802.1AR	RSA, ECC
2	Authentication and Key Establishment	EAP: Extensible Authentication Protocol (EAP-TLS, Cisco EAP-FAST)	IEEE 802.1X (RFC 5126, RFC 4851)	TLS Based: RSA, ECC, AES, HMAC-SHA2
3	Control Key Management	MKA: MACsec KEY Agreement	IEEE 802.1X-2010	AES-128 KeyWrap, AES-128-CMAC AES-256-CMAC
4	Authorization and Key Distribution	RADIUS with Cisco Key Wrap Attributes	RFC 6218	AES-128-KeyWrap, HMAC-SHA-2 DTLS IPSec
5	Bulk Data Encryption	MACsec	IEEE 802.1 AE 802.1AEbn 802.1AEbw 802.1AEcg	AES-GCM-128 AES-GCM-256 AES-GCM-128-XPN AES-GCM-256-XPN

802.1AE (MASec) Tagging

TrustSec Frame Format

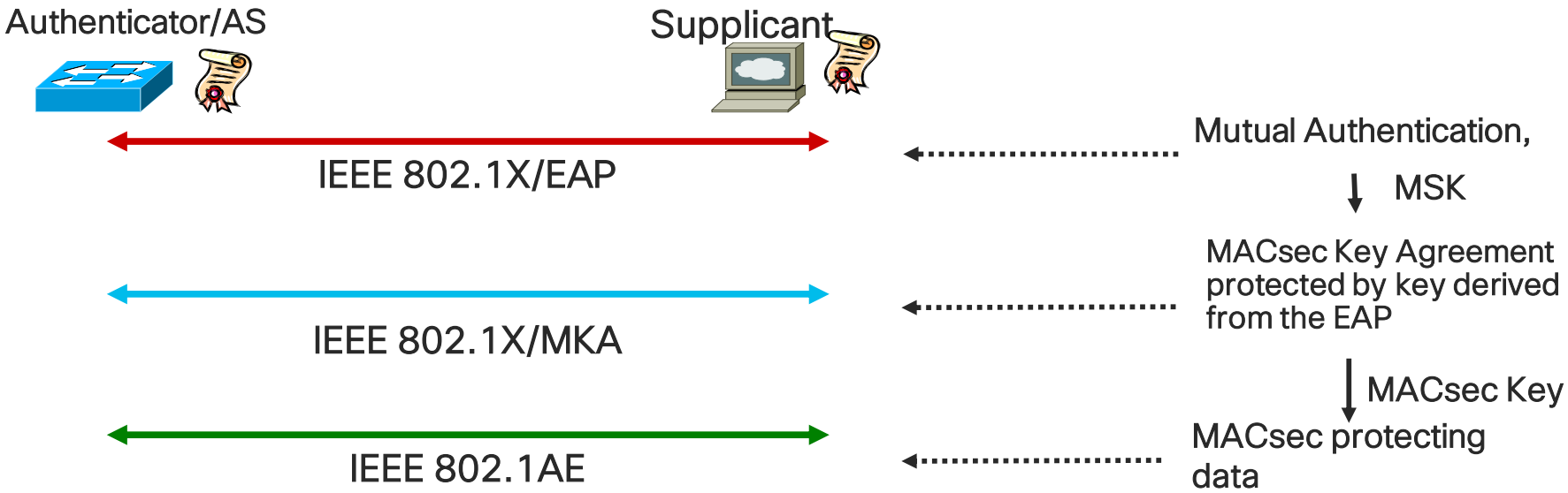


- ✓ Frames are encrypted and protected with an integrity check value (ICV)
- ✓ MACsec Ethertype is 0x88e5
- ✓ No impact to IP MTU/Fragmentation
- ✓ L2 Frame MTU Impact*: ~ 40 bytes = less than baby giant frame (~1600 bytes with 1552 bytes MTU)

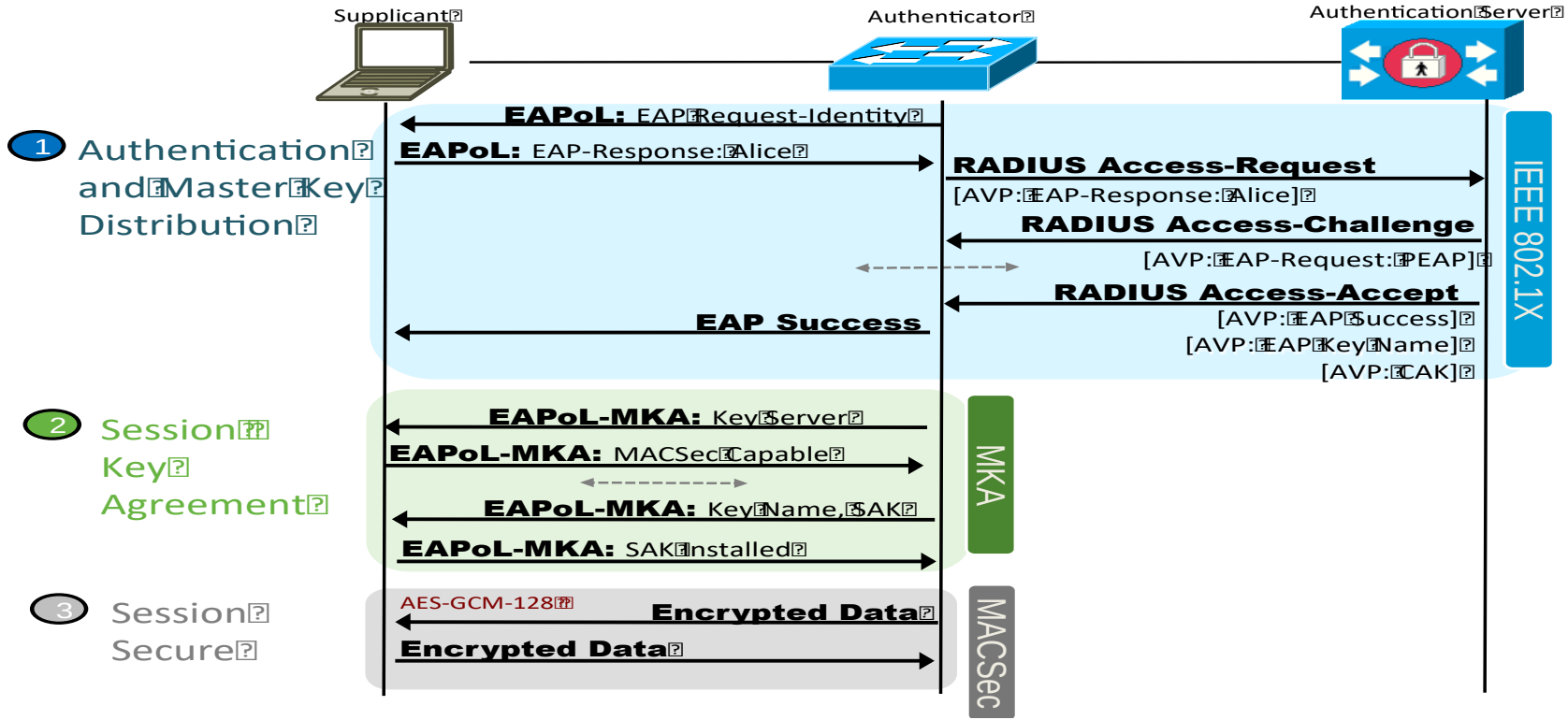
Quick MACsec Terminology

Acronym	Definition
MKA	MACsec Key Agreement – defined in IEEE 802.1XREV-2010 is a key agreement protocol for discovering MACsec peers and negotiating keys
MSK	Master Session Key, generated during EAP exchange. Supplicant and authentication server use the MSK to generate the CAK.
CAK	Connectivity Association Key is derived from MSK. CAK is a long-lived master key used to generate all other keys used for MACsec.
CKN	Connectivity Association Key Name – identifies the CAK
SAK	Secure Association Key is derived from the CAK and is the key used by supplicant and switch to encrypt traffic for a given session.
KS	Key Server • responsible for selecting and advertising a cipher suite • responsible for generating the SAK from the CAK.

MACsec Key Agreement (MKA) and EAP Authentication

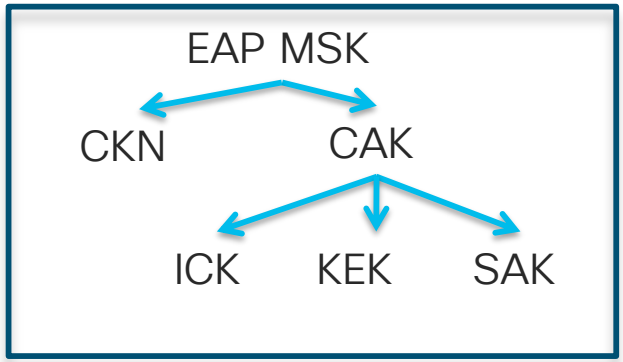


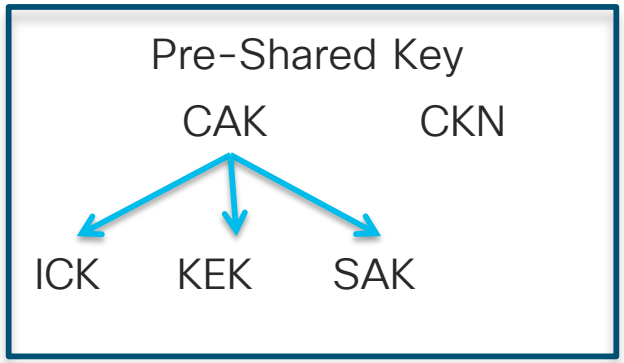
MACsec Functional Sequence



MACsec Key Hierarchy

- Two Methods to derive Encryption Keys
  - 802.1X/EAP
  - Pre-shared Keys
- If EAP method is used – all keys are generated from the Master Session Key (MSK)
- If Pre-shared Key is used the CAK=PSK and the CKN must be manually entered



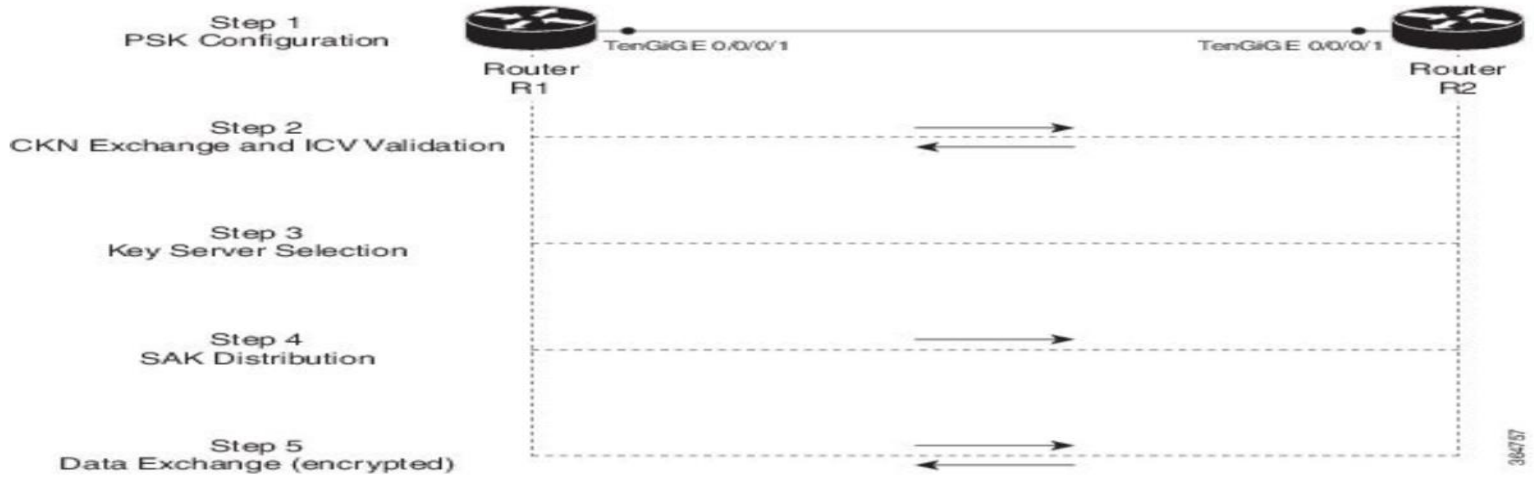


MKA with Pre-shared and cached CAKs

- When EAP is not used for Authentication – a pre-shared key (PSK) can be used.

  The CAK is manually placed in the router/switch configuration and used as the PSK

- Some EAP/MACsec use cases require the link to come up even if the AAA server cannot be reached
  - A preinstalled CAK can be cached in the configuration, and then used until such time as the AAA server is reached and a new CAK is obtained.



Cryptography: Keys used in MKA (CAK/CKN)

- MKA uses a key hierarchy based on a single long-term key (CAK)
  - CAK is derived from the EAP MSK using a key derivation function (KDF) defined in NIST SP800-108. The following is for a 128-bit CAK. (The key is longer for a 256-bit CAK.)

    CAK = KDF(MSK[0-15], "IEEE8021 EAP CAK", mac1 | mac2, CAKlength)

- A unique name is derived for the CAK, called a CKN. This is like a KeyID

  CKN = KDF(MSK[0-15], "IEEE8021 EAP CKN", mac1 | mac2, CKNlength)

Note: A pre-shared or cached CAK requires both the CAK and CKN to be saved in the network device configuration, as well as some policy (e.g., cipher suite)

Keys used in MKA (MKA keys/SAK)

- Two keys are generated from the CAK by MKA
  - ICV Key (ICK) used to prove an authorized peer sent the message
  - ICK = KDF(CAK, “IEEE8021 ICK”, Keyid, ICKLength)
  - Key Encrypting Key (KEK) used to protect the MACsec keys (SAK)
  - KEK = KDF(CAK, “IEEE8021 KEK”, Keyid, KEKLength)
- A MACsec key is called a Secure Association Key (SAK)
  - It is typically generated using the KS FIPS 140-2 compliant random number generator
  - Alternatively, it can be generated using a KDF, including randomness provided by other participants as well as the KS. This protects against a failure in KS randomness

    SAK = KDF(CAK, “IEEE8021 SAK”, KS-nonce | MI-value list | KN, SAKlength)

    Where:
    - KS-nonce is randomness provided by the KS,
    - MI-value list includes a 32-bit value provided by each member in the group (not the MAC address)
    - KN is a counter maintained by the KS

Let's talk MACsec Access Control

- Use the **macsec access-control** {**must-secure** | **should-secure**} command to control the behavior of unencrypted packets.
- The **should-secure** keyword allows unencrypted packets from the physical interface or subinterfaces to be transmitted or received.
- The **must-secure** keyword does not allow unencrypted packets from physical interface or subinterfaces to be transmitted or received. All such packets are dropped except for MKA control protocol packets

CAUTION

- If MACsec is enabled only on selected subinterfaces, configure the **should-secure** keyword option on the corresponding interface.
- The default configuration for MACsec on subinterfaces is **macsec access-control must-secure**. This option is enabled by default when the **macsec** command is configured on an interface.

MKA Key Chain configuration

```
key chain June-key macsec
 key 01
   cryptographic-algorithm aes-128-cmac
  key-string 12345678901234567890123456789011
   lifetime 00:00:00 Jun 1 2017 23:59:59 Jun 30 2017
key chain KEY_1 macsec
 key 01
   cryptographic-algorithm aes-256-cmac
  key-string 1234567890123456789012345678901212345678901234567890123456789012
   lifetime 00:00:00 Jan 1 2015 infinite
 key 10
   cryptographic-algorithm aes-128-cmac
   lifetime 00:00:00 Jan 1 2016 00:00:00 Jan 1 2017
key chain key-roll macsec
 key 01
   cryptographic-algorithm aes-128-cmac
  key-string 12345678901234567890123456789012
   lifetime 14:59:59 Apr 4 2017 duration 5000
 key 02
   cryptographic-algorithm aes-128-cmac
  key-string 12345678901234567890123456789011
   lifetime 16:00:00 Apr 4 2017 17:10:00 Apr 4 2017
```

Key Chain Name

Connectivity Association Key Name (CKN)

MKA Authentication Cipher

Connectivity Association Key (CAK)

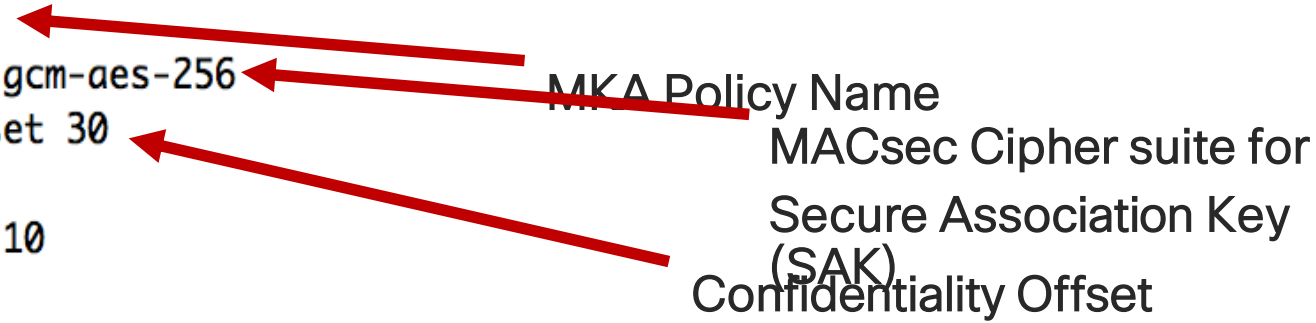
- 32 Characters for 128bit
- 64 Characters for 256bit

Lifetime

Note: The lifetime is for the CKN not the CAK

MKA Policy

```
mka policy POLICY_1
 macsec-cipher-suite gcm-aes-256
 confidentiality-offset 30
mka policy policy2
 key-server priority 10
 delay-protection
 macsec-cipher-suite gcm-aes-256
 confidentiality-offset 30
```

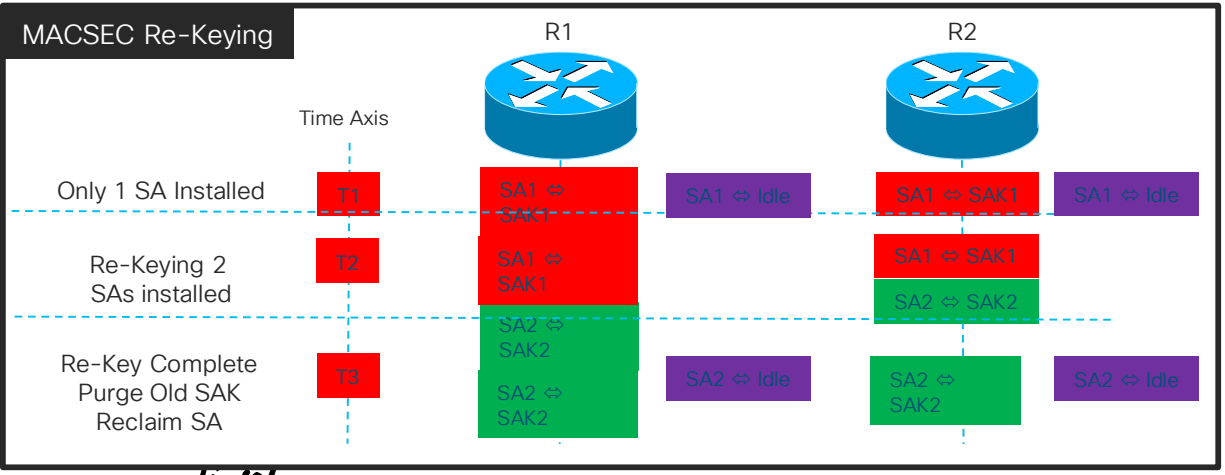


MACSec Interface Configuration

```
interface TenGigabitEthernet0/0/1
 description WAN MACsec Trunk (to ASR 1000 B)
 mtu 2000
 ip address 10.5.0.1 255.255.255.0
 ip mtu 1468
 eapol destination-address broadcast-address
 mka policy POLICY_1
 mka pre-shared-key key-chain key-roll
 macsec
 cdp enable
```

MACSEC SA Scale with Re-Keying (ASR9K)

- We always allocate 2 SAs:
  - 1st SA = Active SA has SAK
  - 2nd SA = Idle SA reserved for re-keying, has no SAK
- During re-key time there is time overlap to:
  1. Exchange and install new SAK key and bind it to idle SA
  2. Purge the old SAK key and allocate an new idle SA



AES-GCM-256-bit	Effective Scale with Re-Keying
Total MACSEC Ports Per System	10G = 1,600 40G = 320 100G = 160
Per Port SA Count	10G Tx/Rx SAs = 32/2 = 16 40G Tx/Rx SAs = 128/2 = 64 100G Tx/Rx SAs = 256/2 = 128
Total MACSEC SAs Per System	10G Tx/Rx SAs = 51,200/2 = 25,600 40G Tx/Rx SAs = 40,960/2 = 20,480 100G Tx/Rx SAs = 40,960/2 = 20,480

MACSEC SA Scale with Re-Keying (IOS-XE)

```
key chain key-roll macsec
 key 01
   cryptographic-algorithm aes-128-cmac
  key-string 12345678901234567890123456789012
   lifetime 14:59:59 Apr 4 2017 duration 5000
 key 02
   cryptographic-algorithm aes-128-cmac
  key-string 12345678901234567890123456789011
   lifetime 16:00:00 4 apr 2017 17:10:00 4 apr 2017
key 03
   cryptographic-algorithm aes-128-cmac
  key-string 12345678901234567890123456789013
   lifetime 17:00:00 4 apr 2017 18:10:00 4 apr 2017
 key 04
   cryptographic-algorithm aes-128-cmac
  key-string 12345678901234567890123456789014
   lifetime 18:00:00 4 apr 2017 infinite
```

MACSEC SA Scale with Re-Keying (IOS-XE)

```
ASR-1000-B#
Apr  4 16:00:00.000: %MKA-5-CAK_REKEY: (Te0/0/1 : 8) MKA Session
is beginning a CAK Rekey  for RxSCI b0aa.7741.3f01/0008,
AuditSessionID , AuthMgr-Handle 5F000003, Old CKN
01000000000000000000000000000000000000000000000000000000000000

Apr  4 16:00:00.000: %MKA-4-MKA_MACSEC_CIPHER_MISMATCH: (Te0/0/1 :
8) Lower strength MKA-cipher than macsec-cipher for RxSCI
b0aa.7741.3f01/0000, AuditSessionID , CKN
02000000000000000000000000000000000000000000000000000000000000

Apr  4 16:00:24.367: %MKA-6-SAK_REKEY_SUCCESS: (Te0/0/1 : 8) MKA
Session successfully completed a SAK Rekey (new Latest AN/KN 3/4,
Old AN/KN 2/3) for RxSCI b0aa.7741.3f01/0008, AuditSessionID , CKN
02000000000000000000000000000000000000000000000000000000000000

Apr  4 16:00:24.367: %MKA-5-SESSION_SECURED: (Te0/0/1 : 8) MKA
Session was secured for RxSCI b0aa.7741.3f01/0008, AuditSessionID
, CKN
02000000000000000000000000000000000000000000000000000000000000
```

MKA Info

```
ASR-1000-A# show mka summary

Total MKA Sessions....... 1
      Secured Sessions... 1
      Pending Sessions... 0

=============================================================================================================
Interface       Local-TxSCI          Policy-Name      Inherited        Key-Server
Port-ID         Peer-RxSCI           MACsec-Peers     Status           CKN
=============================================================================================================
Te0/0/1         b0aa.7741.3f01/0008 POLICY_1         NO               NO
8               80e0.1d27.2101/0008 1                Secured          040000000000000000000000000000000000000000000000
```

```
ASR-1000-A#show mka keychains

MKA PSK Keychain(s) Summary...

Keychain          Latest CKN                                                          Interface(s)
Name              Latest CAK                                                          Applied
=============================================================================================================
KEY_1             010000000000000000000000000000000000000000000000000000000000000000 Gi0/0/1.10     Gi0/0/0
                  <HIDDEN>

key-roll          040000000000000000000000000000000000000000000000000000000000000000 Te0/0/1
                  <HIDDEN>
```

MACSec Status

```
ASR-1000-A#show macsec status in tenGigabitEthernet 0/0/1
 Capabilities:
  Ciphers Supported:        GCM-AES-128 GCM-AES-256
  Cipher:                   GCM-AES-256
  Confidentiality Offset:   30
  Replay Window:            64
  Delay Protect Enable:     FALSE
  Access Control:           must-secure

 Transmit SC:
  SCI:                      B0AA77413F010008
  Transmitting:             TRUE
 Transmit SA:
  Next PN:                  98171
  Delay Protect AN/nextPN:  99/0

 Receive SC:
  SCI:                      80E01D2721010008
  Receiving:                TRUE
 Receive SA:
  Next PN:                  98199
  AN:                       0
  Delay Protect AN/LPN:     0/0
```

Prerequisites for Certificate-based MACsec Encryption

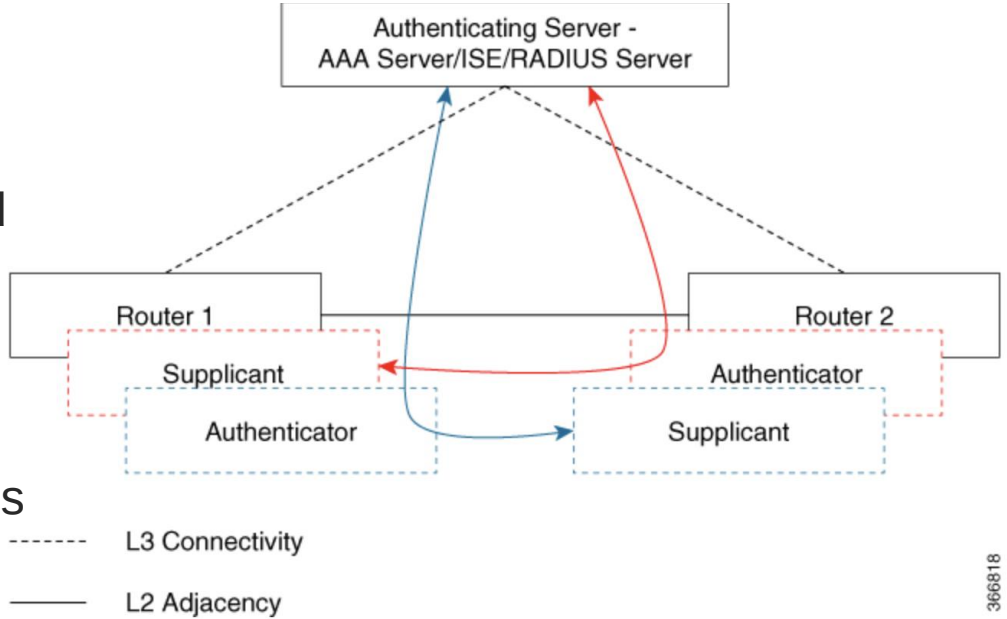
- Ensure that you have a Certificate Authority (CA) server configured for your network.
- Generate a CA certificate.
- Ensure that you have configured Cisco Identity Services Engine (ISE) Release 2.0. Refer to the *Cisco Identity Services Engine Administrator Guide, Release 2.3*.
- Ensure that both the participating devices, the CA server, and Cisco Identity Services Engine (ISE) are synchronized using Network Time Protocol (NTP). If time is not synchronized on all your devices, certificates will not be validated.
- Ensure that 802.1x authentication and AAA are configured on your device.

Restrictions for Certificate-based MACsec Encryption

- MKA is not supported on port-channels.
- High Availability for MKA is not supported.
- Certificate-based MACsec encryption on sub-interfaces is not supported.

Call Flow for Certificate-based MACsec Encryption using Remote Authentication

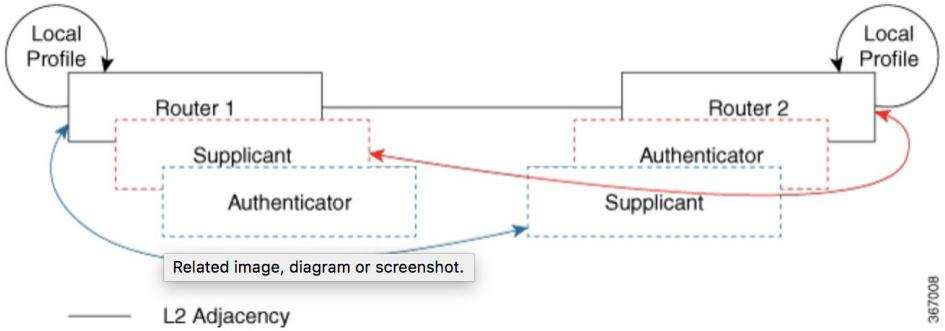
1. MACSec enabled routers will act as both Supplicant and Authenticator
2. Two EAP Sessions (with separate EAP Session IDs) are initiated Red and Blue
3. After mutual authentication, the MSK of the flow corresponding to the router with the higher MAC address and role as authenticator is picked to derive the CAK.



CAK = KDF(MSK[0-15], "IEEE8021 EAP CAK", mac1 | mac2, CAKlength)
CKN = KDF(MSK[0-15], "IEEE8021 EAP CKN", mac1 | mac2, CKNlength)

Call Flow for Certificate-based MACsec Encryption using Local Authentication

1. MACSec enabled routers will act as both Supplicant and Authenticator
2. Two EAP Sessions (with separate EAP Session IDs) are initiated Red and Blue
3. After mutual authentication, the MSK of the flow corresponding to the router with the higher MAC address and role as authenticator is picked to derive the CAK.



CAK = KDF(MSK[0-15], "IEEE8021 EAP CAK", mac1 | mac2, CAKlength)
CKN = KDF(MSK[0-15], "IEEE8021 EAP CKN", mac1 | mac2, CKNlength)

Certificate Based MACSec Configuration .1X Config

```
aaa new-model
dot1x system-auth-control
radius server ISE
  address ipv4 <ISE ipv4 address> auth-port 1645 acct-port 1646 automate-tester
  username dummy
  key dummy123
  radius-server deadtime 2
aaa group server radius ISEGRP
   server name ISE
aaa authentication dot1x default group ISEGRP
 aaa authorization network default group ISEGRP
```

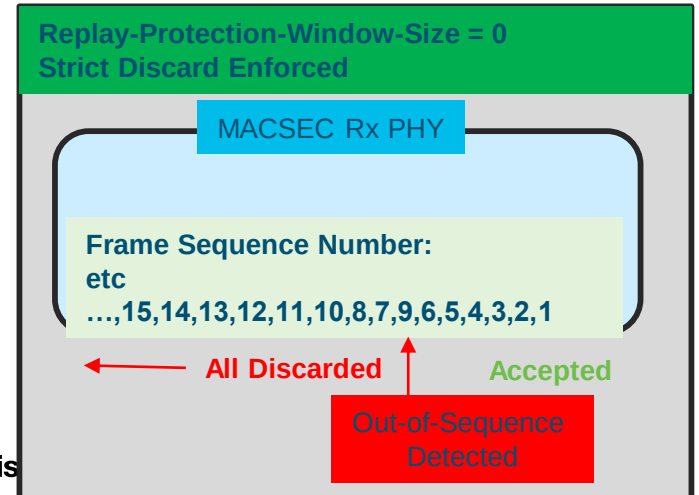
```
eap profile EAPTLS-PROF-IOSCA
        method tls
        pki-trustpoint IOS-CA


dot1x credentials EAPTLSCRED-IOSCA
        username asr1000@cisco.com
        pki-trustpoint IOS-CA !
```

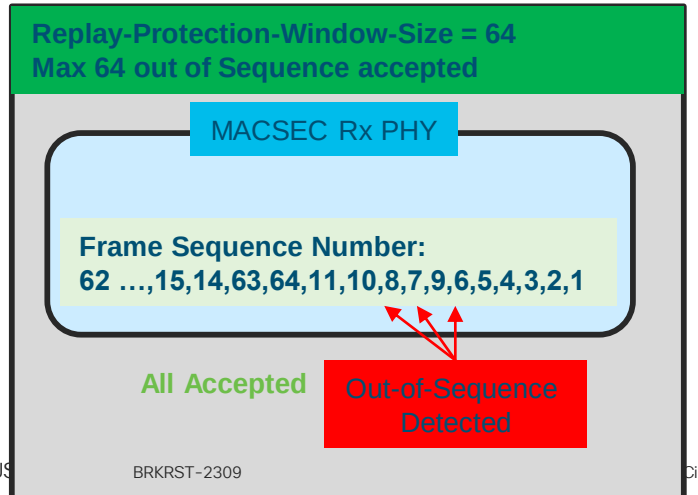
Applying configuration to Interface

```
interface TenGigabitEthernet0/1
 macsec network-link
 authentication periodic authentication timer reauthenticate <reauthentication interval>
 access-session host-mode multi-host
 access-session closed
 access-session port-control auto
 dot1x pae both
 dot1x credentials EAPTLSCRED-IOSCA
 dot1x supplicant eap profile EAPTLS-PROF-IOSCA
 service-policy type control subscriber DOT1X_POLICY_RADIUS
```

Handing MACSEC Out-of-Sequence Frames
Replay-Protection-Window-Size Behavior

- Replay protection Window Size = Maximum out-of-sequence frames MACSEC accepts and not discarded
- MACSEC Egress Decryption PE expects:
  - All frames to be received in sequence as 1,2,3, etc … (ascending order)
  - All out-or-order or out-of-sequence frames should not exceed “Replay Protection Window Size”
  - If any frame with sequence number outside of window size arrives it will be discarded. Eg, window expects 1-64, but we get 100 then100 will be discarded.





WHY AES-GCM-XPN?

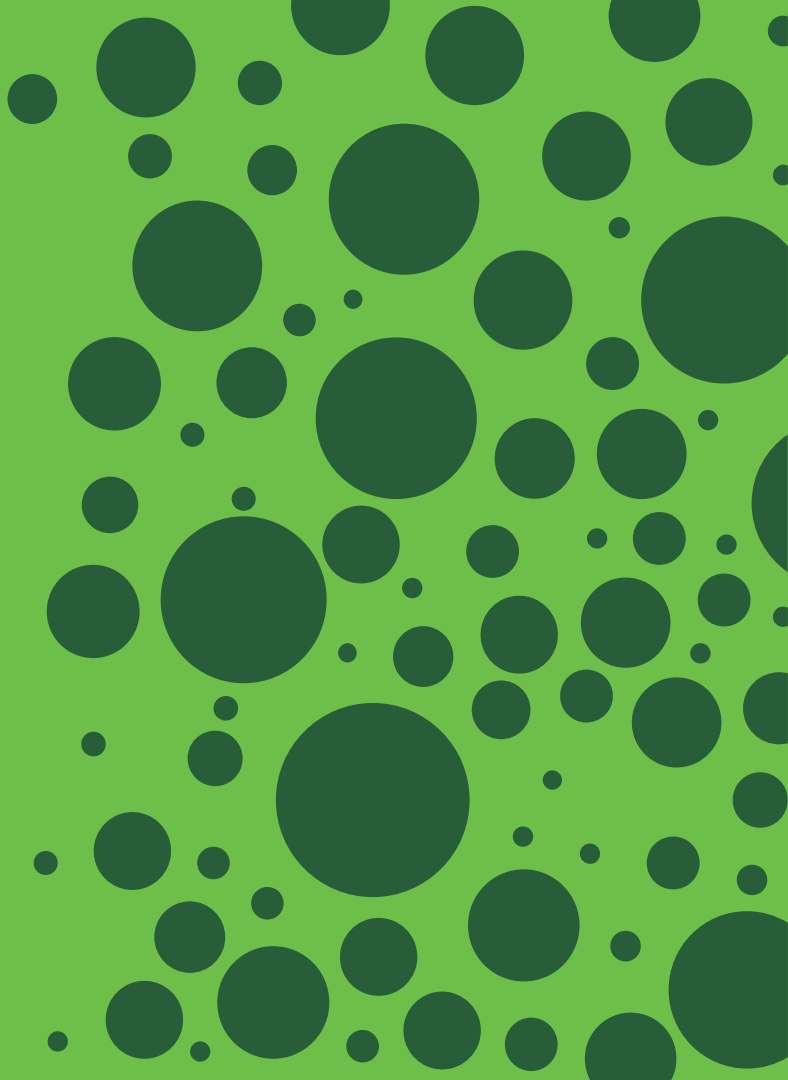
Packet Size	1,000,000,000	Rekey Timer			10,000,000,000	Rekey Timer			40,000,000,000	Rekey Timer			100,000,000,000	Rekey Timer		
	1GE Rate	Seconds	Minutes		10GE Rate	Seconds	Minutes		40GE Rate	Seconds	Minutes		100GE Rate	Seconds	Minutes	
64	1,488,095	1,443	24		14,880,952	144	2.4		59,523,810	36	0		148,809,524	14	0.2	
256	452,899	4,742	79		4,528,986	474	7.9		18,115,942	119	2		45,289,855	47	0.8	
512	234,962	9,140	152		2,349,624	914	15.2		9,398,496	228	3.8		23,496,241	91	1.5	
1024	119,732	17,936	299		1,197,318	1,794	29.9		4,789,272	448	7.5		11,973,180	179	3.0	

Packet Size	1,000,000,000	Rekey Timer			10GE	Rekey Timer			40,000,000,000	Rekey Timer			100,000,000,000	Rekey Timer		
	1GE Rate	Seconds	Minutes	Days	10GE Rate	Seconds	Minutes	Days	40GE Rate	Seconds	Minutes		100GE Rate	Seconds	Minutes	Days
64	1,488,095	6,198,106,008,766	103,301,766,813	71,737,338	14,880,952	619,810,600,877	10,330,176,681	7,173,734	59,523,810	154,952,650,219	2,582,544,17	1,793,433	148,809,524	61,981,060,088	1,033,017,668	717,373
256	452,899	20,365,205,457,375	339,420,090,956	235,708,396	4,528,986	2,036,520,545,738	33,942,009,096	23,570,840	18,115,942	509,130,136,434	8,485,502,2	5,892,710	45,289,855	203,652,054,574	3,394,200,910	2,357,084
512	234,962	39,254,671,388,854	654,244,523,148	454,336,474	2,349,624	3,925,467,138,885	65,424,452,315	45,433,647	9,398,496	981,366,784,721	16,356,113,07	11,358,412	23,496,241	392,546,713,889	6,542,445,231	4,543,365
1024	119,732	77,033,603,251,811	1,283,893,387,530	891,592,630	1,197,318	7,703,360,325,181	128,389,338,753	89,159,263	4,789,272	1,925,840,081,295	32,097,334,688	22,289,816	11,973,180	770,336,032,518	12,838,933,875	8,915,926

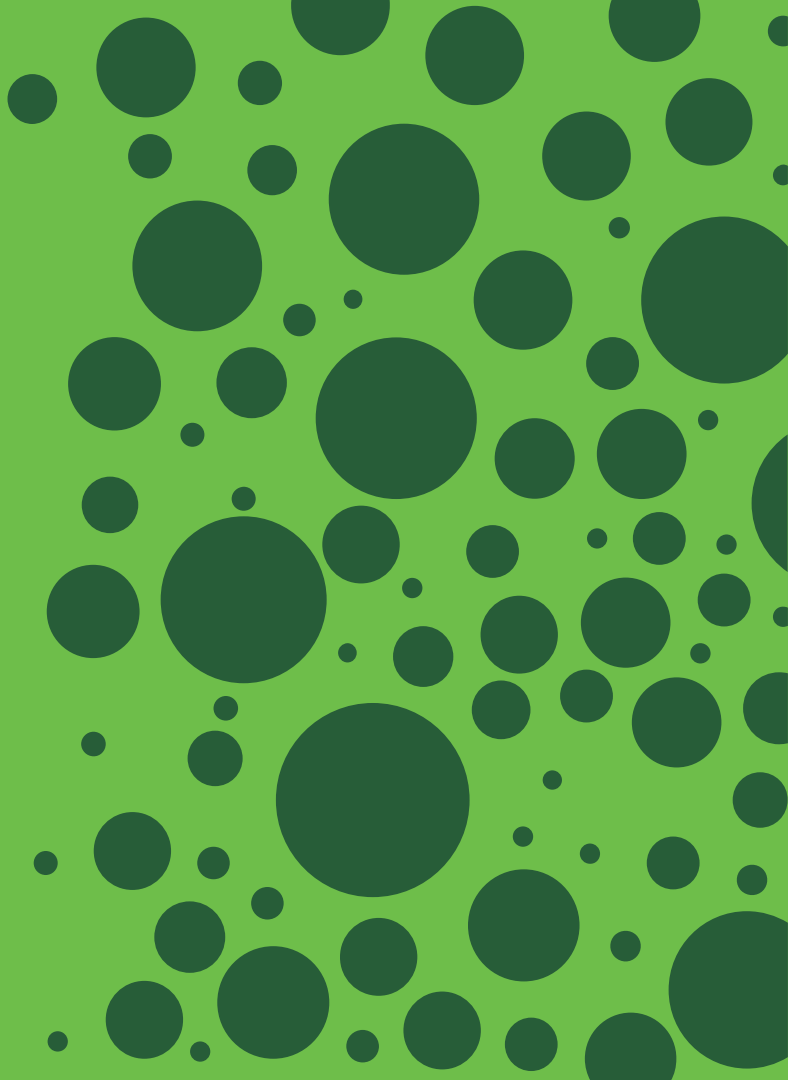
MACsec and IPsec Comparison

Category	MACsec	IPsec
Market Positioning	1. Aggregate Deployments such as Regional Hubs 2. Large Branches that require high throughput 3. Data Center Interconnects	1. Small Branches 2. High Scale deployments 3. Low throughput Branches 4. Beyond MetroE (International) Reach
Link Requirement/Topologies	Requires dedicated MetroE EVC circuits for L2 connectivity between sites Point-to-Point, Point-to-MultiPoint	Easily Routable over many commonly available public network Any Topology
Encryption Performance	Per PHY Link Speed (1G, 10G, 40G, 100G)	Constrained by IPsec Crypto engine performance
Services Enablement	No impact to encryption throughput	Impacts encryption throughput
Peers Scale	Limited by hardware resources	Highly Scalable
Throughput	Up to Line Rate on each port (limited only by the forwarding capability)	Aggregate throughput (limited by the encryption throughput)
Configurability	Simple configuration	More complex configuration and policy choices
Layer 3 Visibility for Monitoring	No. Except Layer 2 headers (and optionally VLAN/MPLS Labels) everything else is encrypted	Visible. L3 info can be used for monitoring & policy enforcement purposes

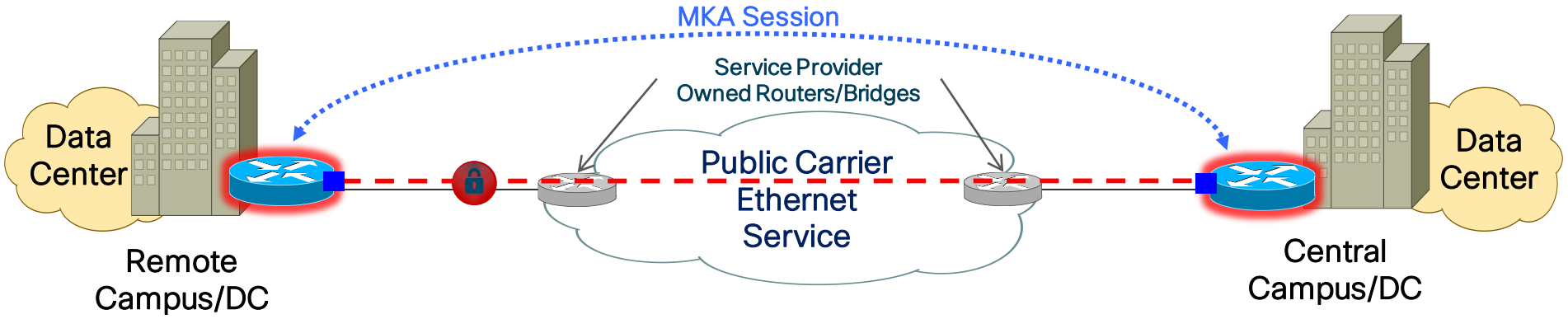
MACsec Deployment Models and Use Cases



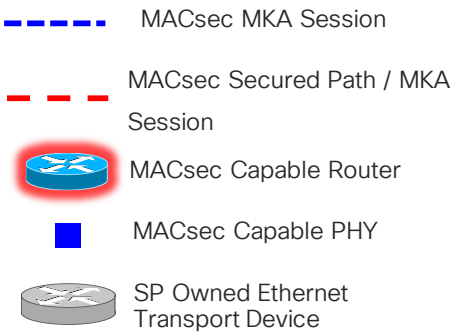
What is WAN MACsec?



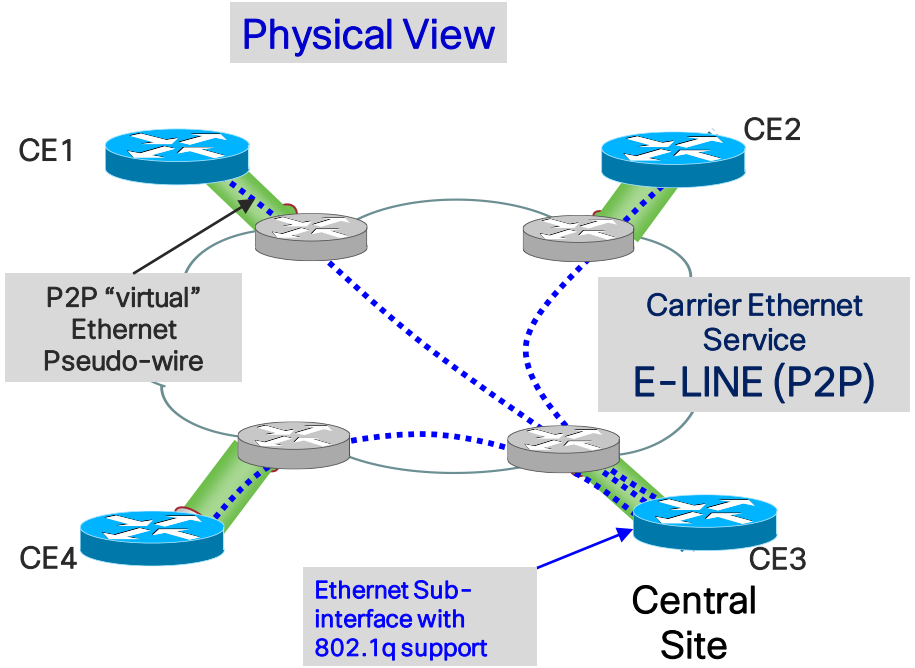
What is “WAN MACsec?
Secure Ethernet Link(s) over Public Ethernet Transport

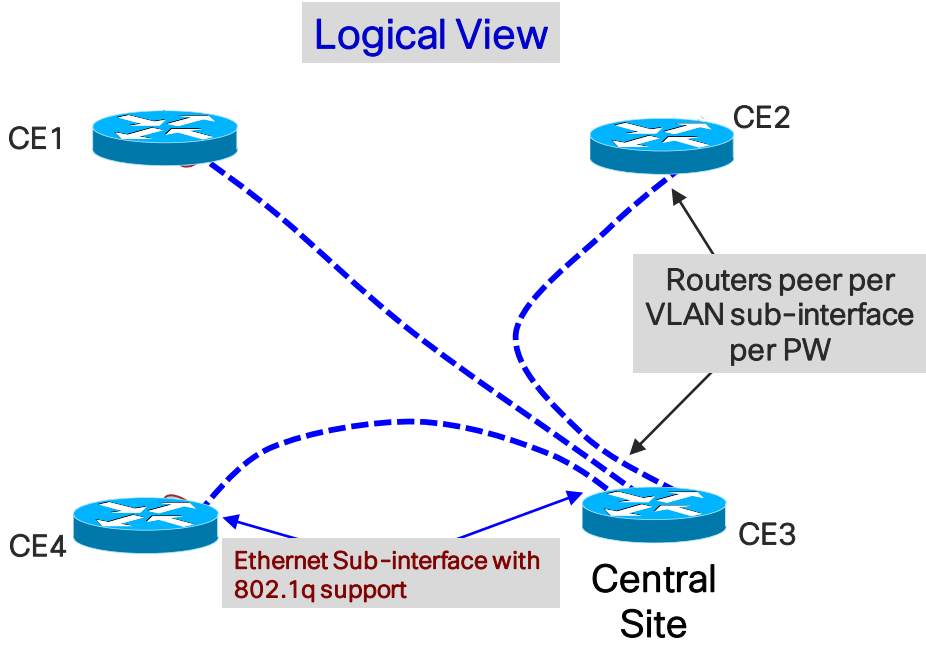


- Leverage “public” standard-based Ethernet transport
- Optimize MACsec + WAN features to accommodate running over public Ethernet transport
- Target “line-rate” encryption, regardless of packet size
- Targets 100G, as well as 1/10/40G



Router Peering Model View over E-LINE
Point to Point E-LINE Service

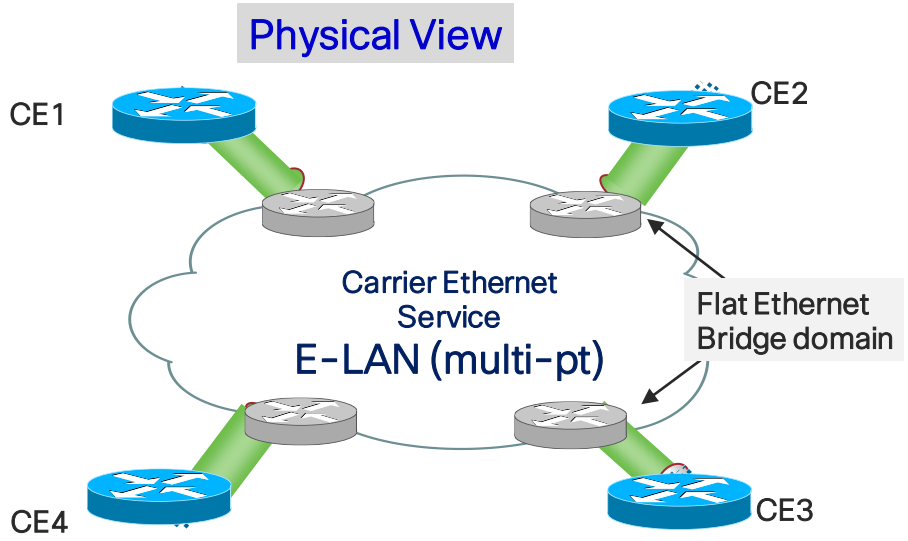


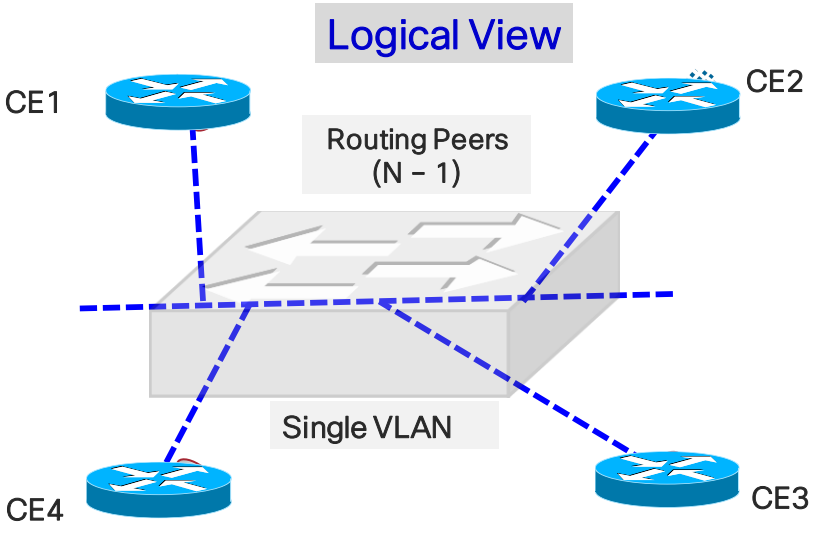


- E-LINE is a point-to-point virtual "Ethernet wire" service
- Connection model can be point to point, with virtual multiplexing at hub site via 802.1Q/sub-interface offering

IP Routing Peer (BGP, Static, IGP)

Router Peering Model View for E-LAN





- E-LAN emulates the network as an "Ethernet switch"
- Routers appear as part of a single "flat" Ethernet domain
- Caution required as IP Peering is N – 1 (N = # of router nodes)
- Transport is MAC address aware of "well known" MAC addresses and Ether types

IP Routing Peer
(BGP, Static, IGP)

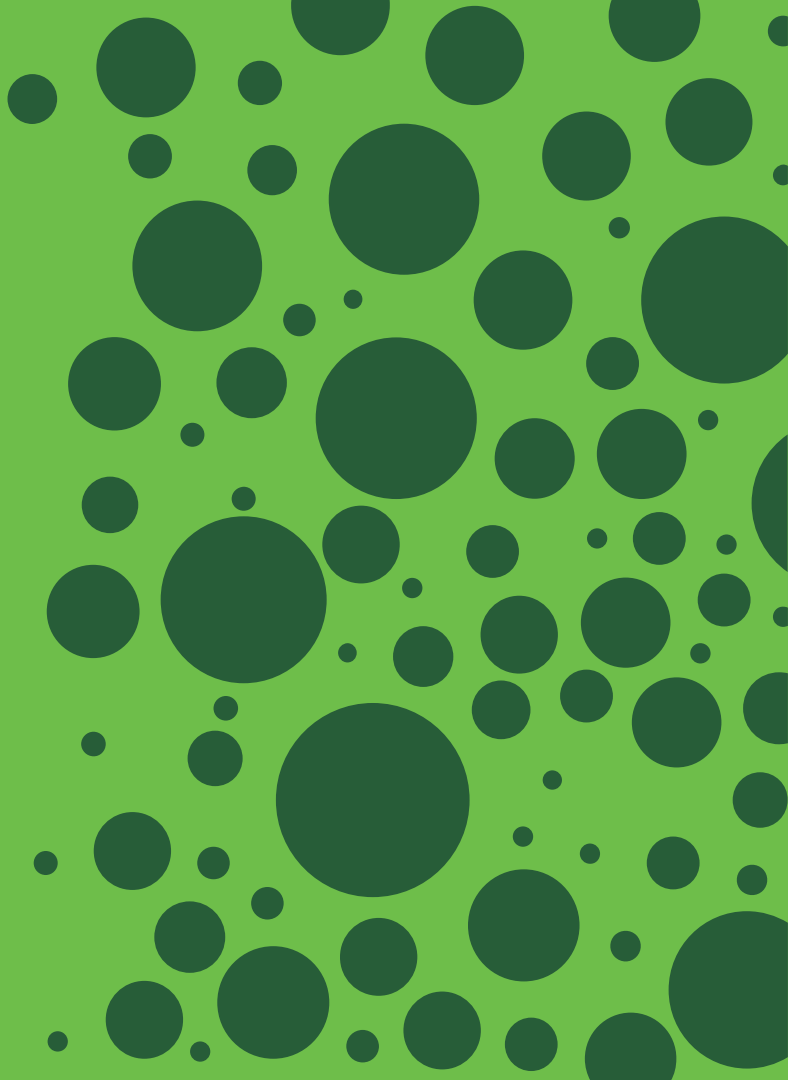
What is “WAN” MACsec?
New Enhancements to 802.1AE for WAN/Metro-E Transport

- AES-256 (AES/GCM) support – 1/10/40 and 100G rates
- Standards Based MKA key framework
  - (defined in 802.1X-2010) within Cisco security
- Ability to support 802.1Q tags in clear
  - Offset 802.1Q tags in clear before encryption (2 tags is optional)
- Vital Network Features to Interoperate over Public Carrier Ethernet Providers
  - **802.1Q tag in the clear**
  - Ability to change **MKA EAPoL Destination Address, Ether-type value**
  - Ability to configure Anti-replay window sizes
- Interoperability among all MACsec platforms in Cisco, Open Standards

MACsec vs. “WAN” MACsec Support

Capability	MACsec	WAN MACsec
Data Plane Encryption	AES-128 (AES-GCM)	AES-128/AES-256 (AES-GCM)
1/10/40/100G AES-256/GCM	No (AES-128 only)	Yes
Control Plane Keying	SAP (Cisco)	MKA (IEEE)
802.1Q Tag in the Clear	No	Yes
Point to MultiPoint Topology	No	Yes
MKA EAPoL Tuning	No	Yes
MKA Ether Type Tuning	No	Yes
Anti Replay Window Support	Limited	Yes
Multi Vendor Support	No	Yes

WAN MACsec Use Cases

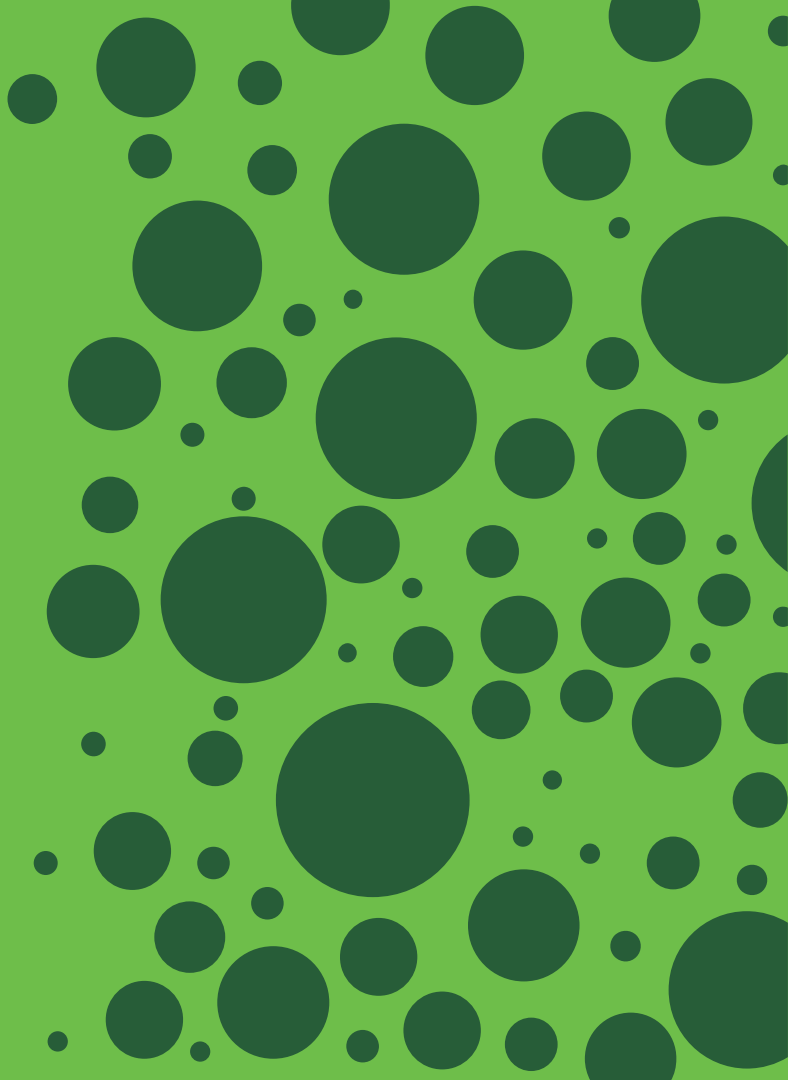


Primary WAN MACsec Use Cases

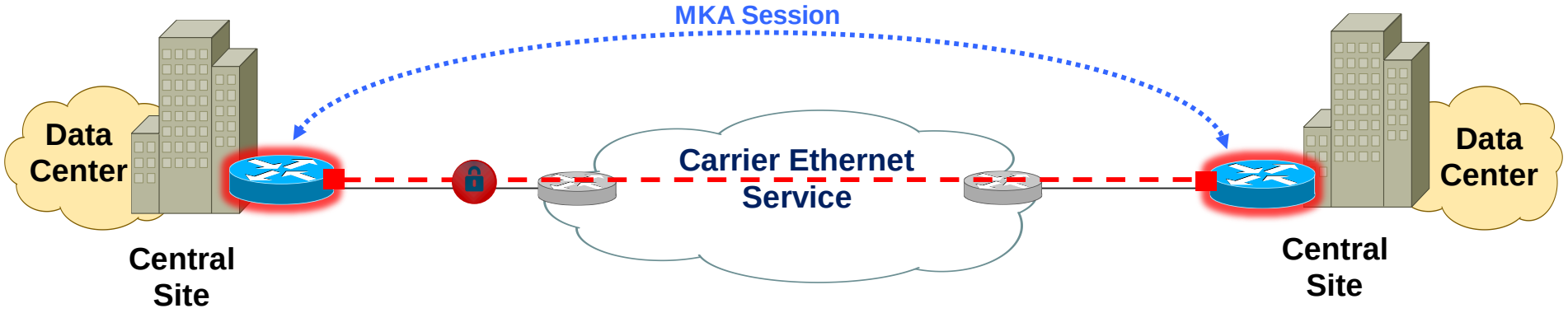
- Point to Point
- Point to Multi Point / Multi-point to Multi-point
- Securing Private IP / MPLS / Segment Routing backbone
- Hybrid Encrypted WAN – WAN MACsec + IPSec

Use Cases

Point to Point Topologies



WAN MACsec Use Cases
High Speed Site to Site

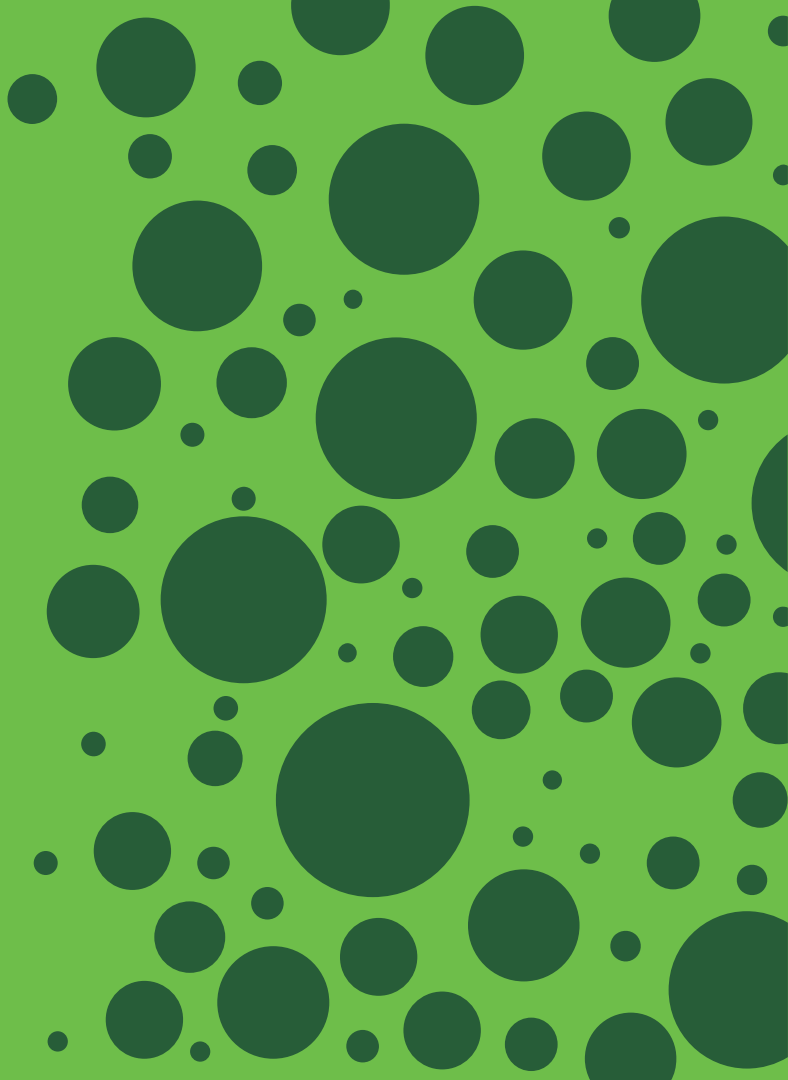


- Point to point PW (EPL) service
- Typically Port-mode, or 802.1Q offering
- Target Solution: High-speed (line-rate) transfers
  - Speeds typically exceed IPSec
  - Reduce IPSec complexity (DMVPN, GRE tunnels)

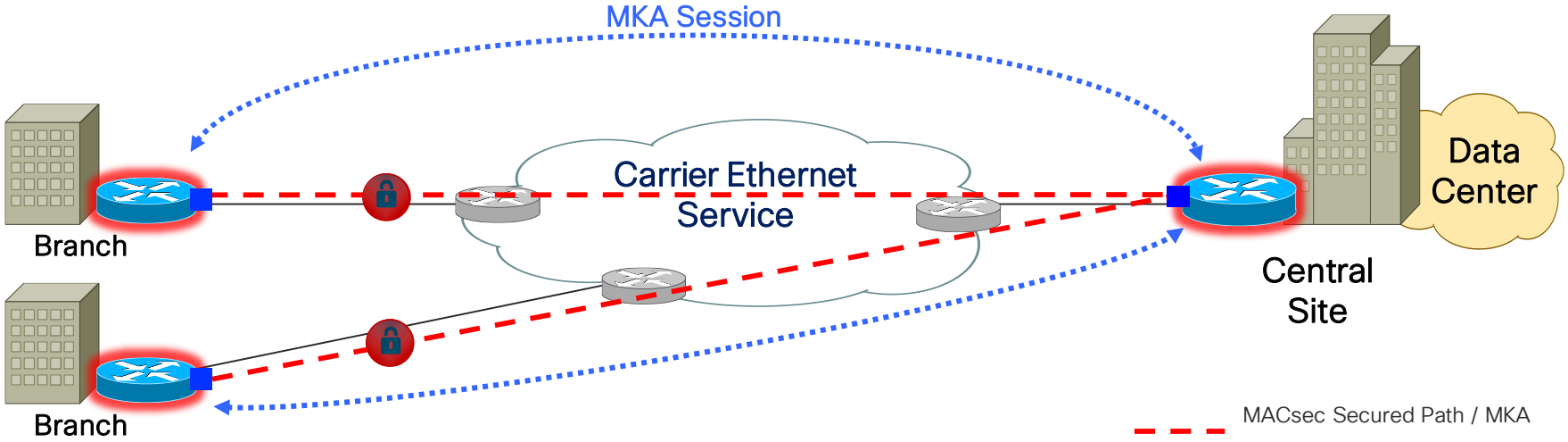
MACsec Secured Path / MKA Session
MACsec Capable Router
MACsec Capable PHY
SP Owned Ethernet Transport Device
MACsec MKA Session

Use Cases

Point to MultiPoint Topologies

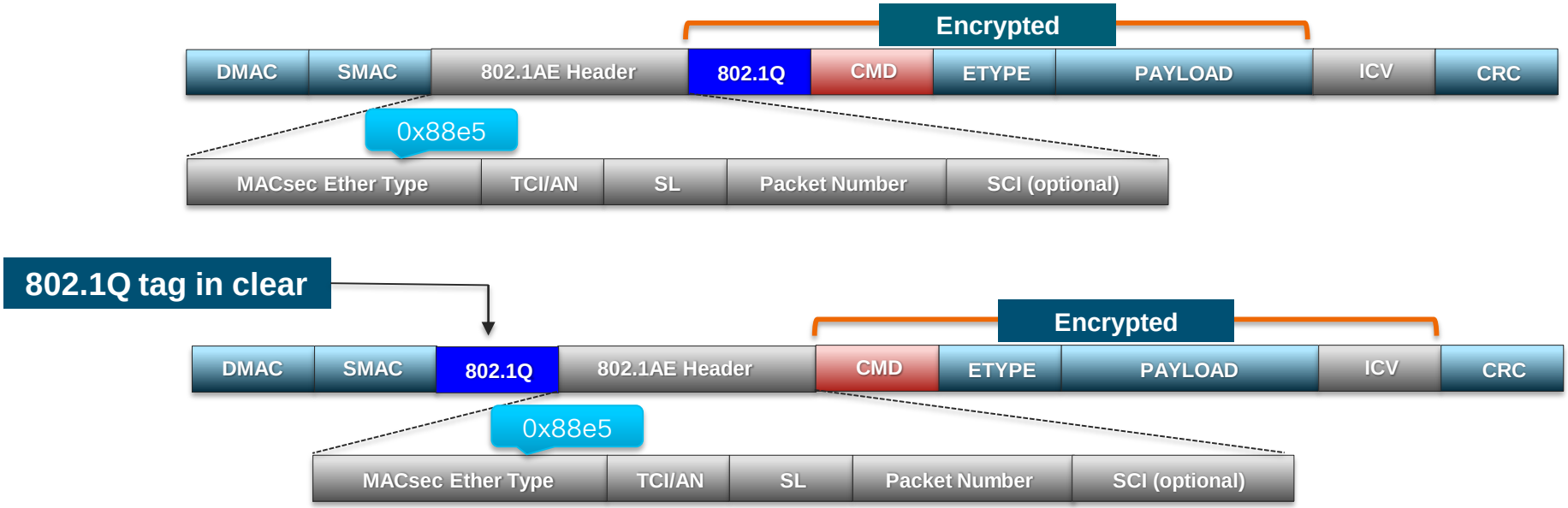


WAN MACsec Use Cases
E-LINE Point to Multipoint Backhaul



- Point to point PW service (no MAC address lookup)
- Must leverage 802.1Q offering at Central site
- Target Solution: Simple and/or high-speed Branch Backhaul
  - Speeds typically exceed IPSec
  - Reduce IPSec complexity (DMVPN, GRE tunnels)

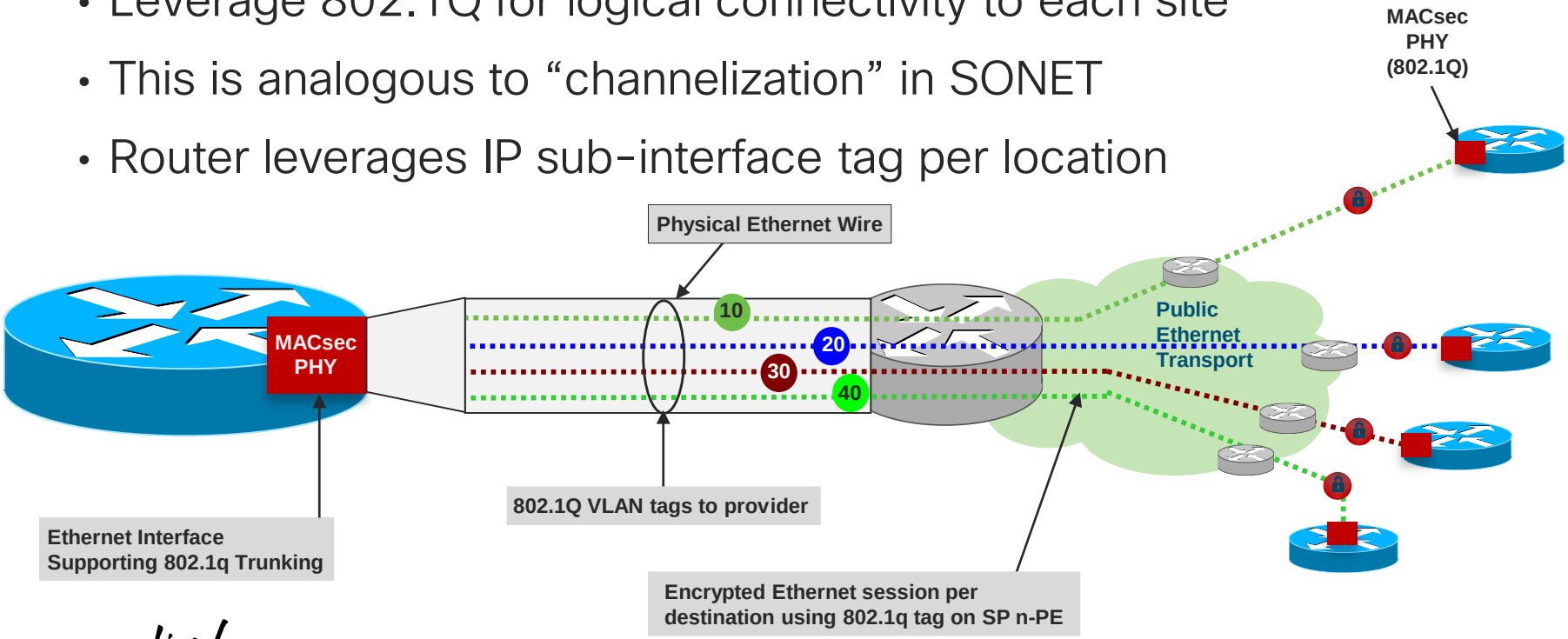
802.1AE (MACsec) “Tag in Clear”



- 802.1Q tag offers significant network design options over the carrier network

WAN MACsec Use Case – 802.1Q Tag in the Clear

- Leverage 802.1Q for logical connectivity to each site
- This is analogous to “channelization” in SONET
- Router leverages IP sub-interface tag per location



WAN MACsec – 802.1Q Tag in the Clear
Expose the 802.1Q tag "outside" the encrypted payload

- Example:

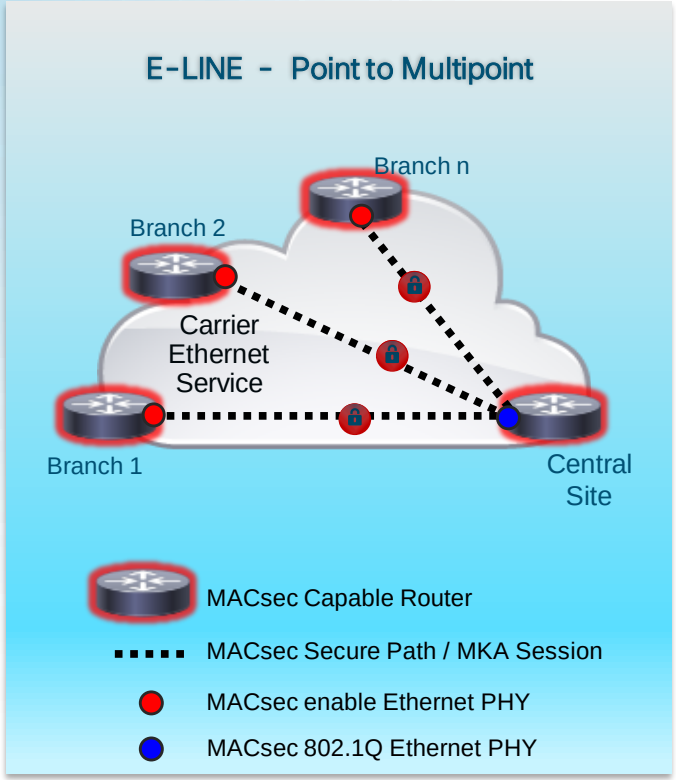
```
...
interface GigabitEthernet0/0/4
  macsec dot1q-in-clear 1

Interface GigabitEthernet0/0/4.20
  encapsulation dot1Q 20
  ip address 10.3.2.1 255.255.255.0
  mka pre-shared-key key-chain k1
  macsec
!
Interface GigabitEthernet0/0/4.30
  encapsulation dot1Q 30
  ip address 10.3.3.1 255.255.255.0
  mka pre-shared-key key-chain k1
  macsec
```

Allows the ability to leverage MACsec on a per sub-interface basis, exposing the "802.1Q tag" outside the encryption header.

Note: "1" denotes one .1Q tag depth

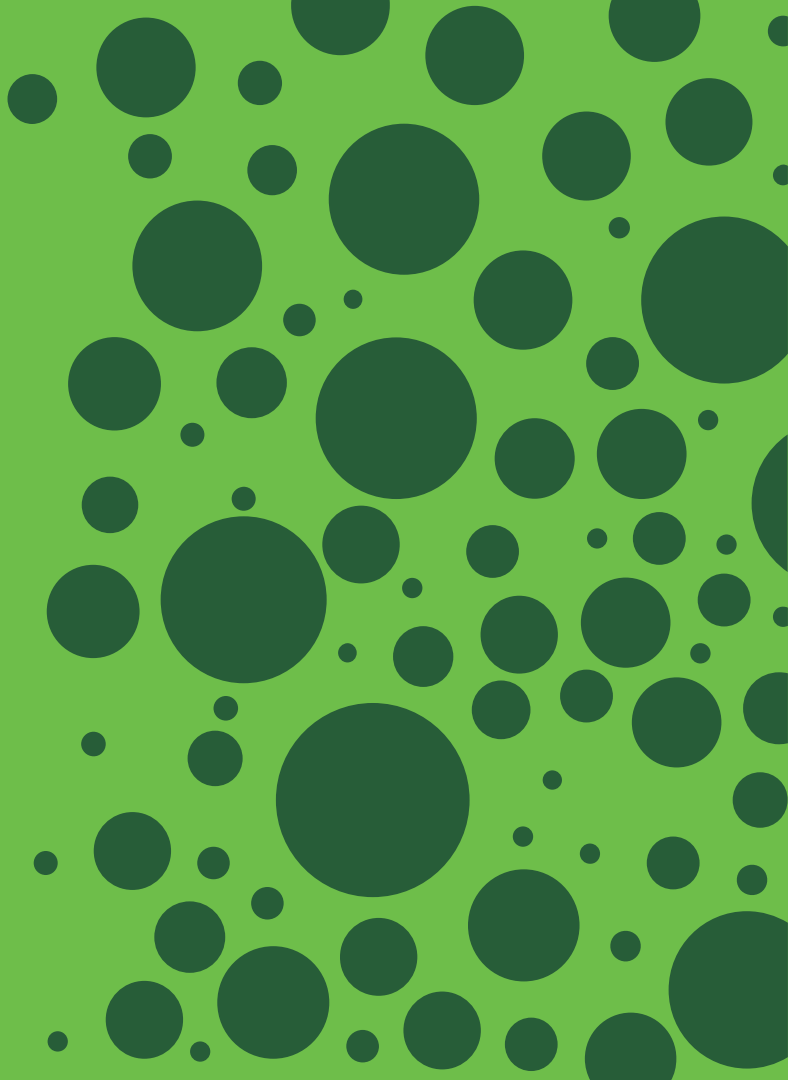
WAN MACsec Use Cases
Point to Multi-point Topology (Hub/Spoke) with 802.1Q Tag in Clear

- Use Case - Requirement
  - High Speed hub-and-spoke Topology Support
  - Leverage low-cost/high-speed Metro E transport
  - Cost Effective Design where N x 10G is required
- WAN MACsec Features
  - Strong Encryption: AES-GCM-256 (Suite B)
  - Leverage 802.1Q in the clear (Hub-Site logical separation)
- Key Benefits
  - Simple to configure
  - Encryption throughput = Router performance (BW/PPS)
  - 802.1Q Tag in Clear allows simple site aggregation
  - Flexible to support MACsec and IPSec at Central Site

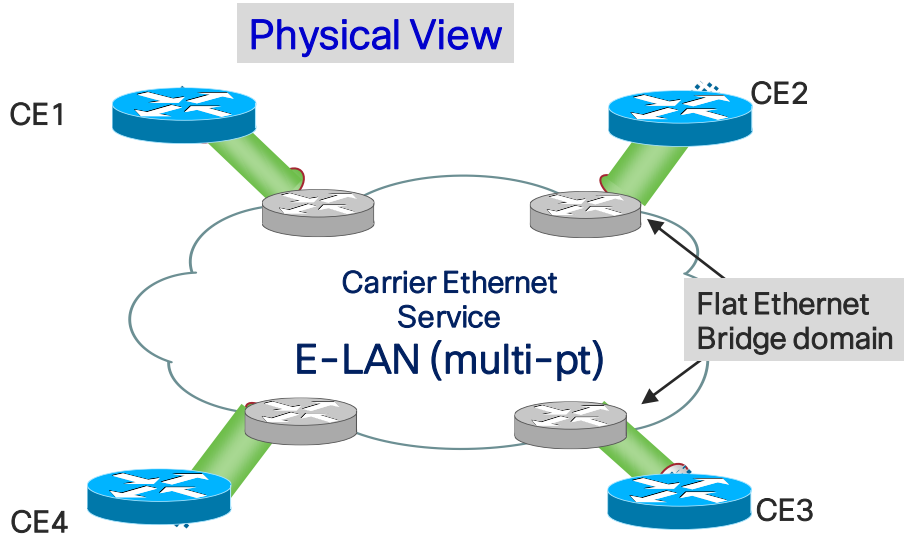


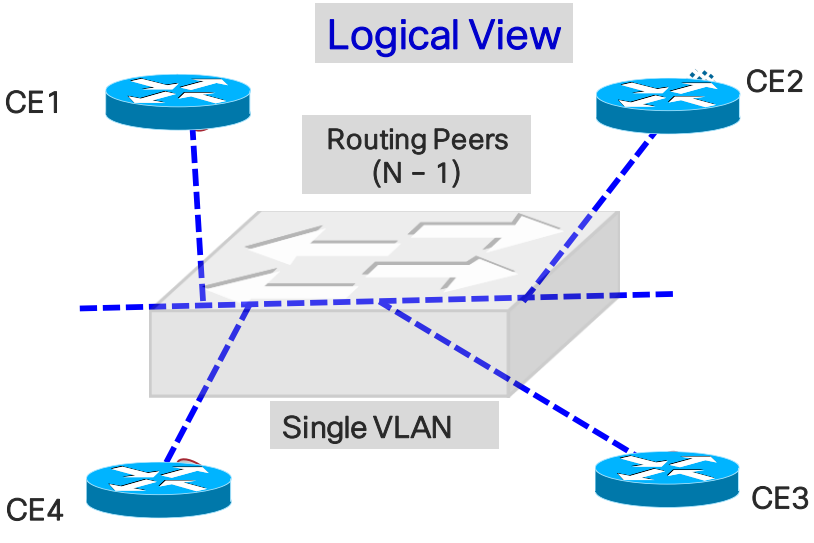
Use Cases

Point to MultiPoint / Multipoint to Multipoint (E-LAN Transport)



Router Peering Model View for E-LAN

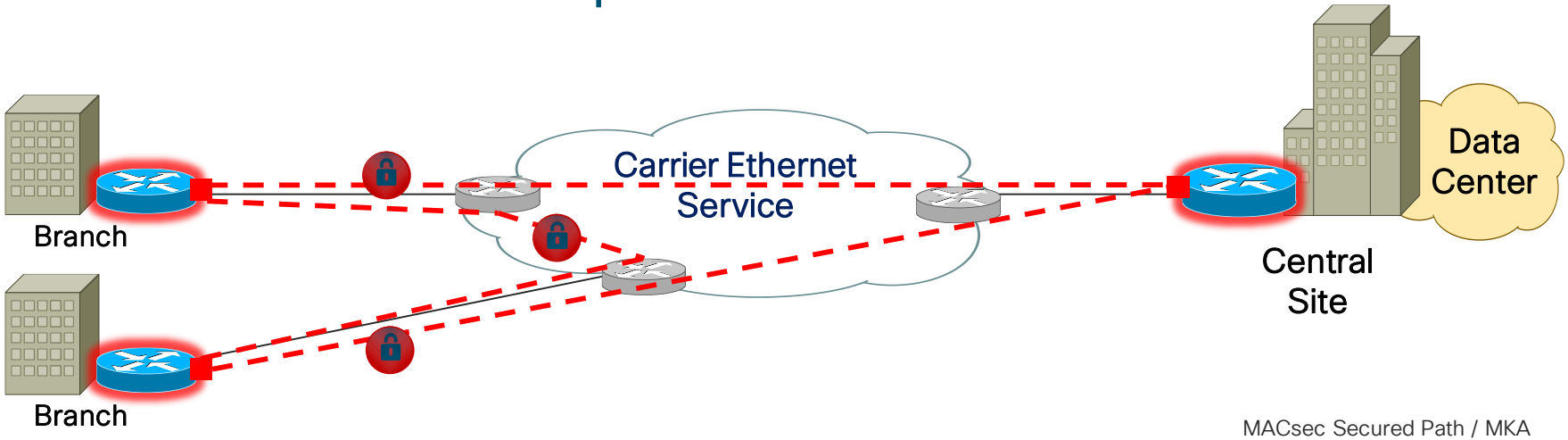




- E-LAN emulates the network as an “Ethernet switch”
- Routers appear as part of a single “flat” Ethernet domain
- Transport is MAC address aware of “well known” MAC addresses and Ether types

IP Routing Peer
(BGP, Static, IGP)

WAN MACsec Use Cases
E-LAN Point to Multipoint Backhaul

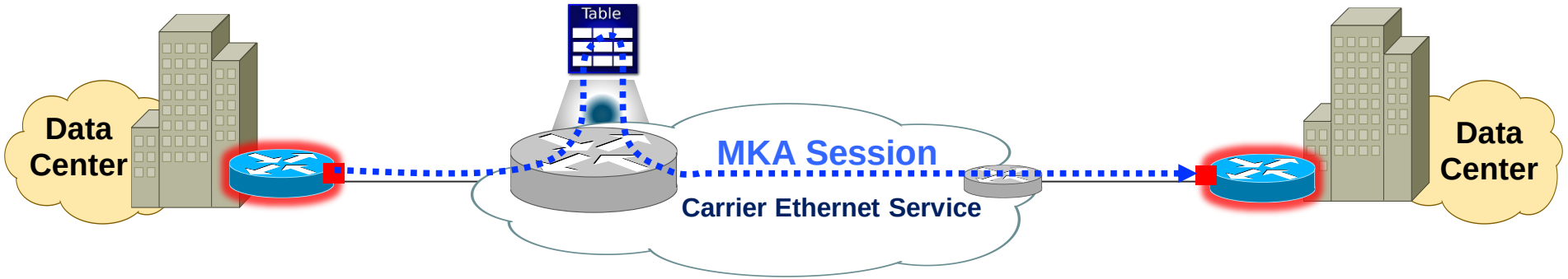


- Transport is based on MAC address lookup
- Option to leverage 802.1Q tags for partial-mesh topology
- Implications – Ethernet provider may consumer (and delete) necessary MKA key exchange packets
  - EAPoL MAC address and Ether-type
- Must allow operator ability to modify EAPoL parameters

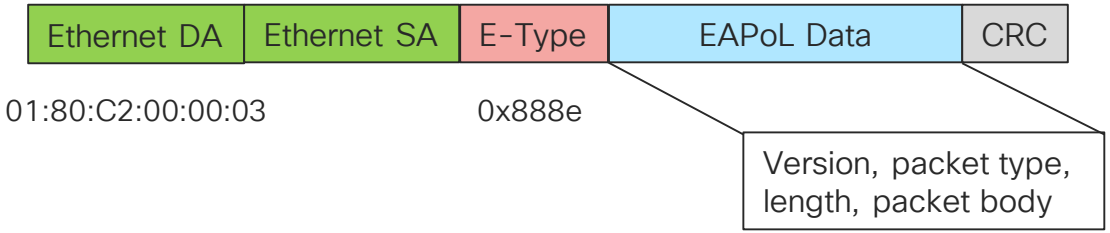
Adapting to Service Provider Ethernet Services
Enhancement: Ability to Change EAPoL Destination Address

- MKA uses Extensible Authentication Protocol over LAN (EAPoL) as the transport protocol
- By default, EAPoL uses a destination multicast MAC address of 01:80:c2:00:00:03
- Because EAPoL is a standards (802.1X), the SP may consume this packet (based on the destination multicast MAC address)
- If so, the EAPoL packet will eventually get dropped, causing the MKA session establishment process to fail
- **We need a method to change the destination MAC address and the ether-type of an EAPoL packet**, to ensures the SP tunnels the packet like any other data packet instead of consuming them.

WAN MACsec Use Cases
High Speed Site to Site

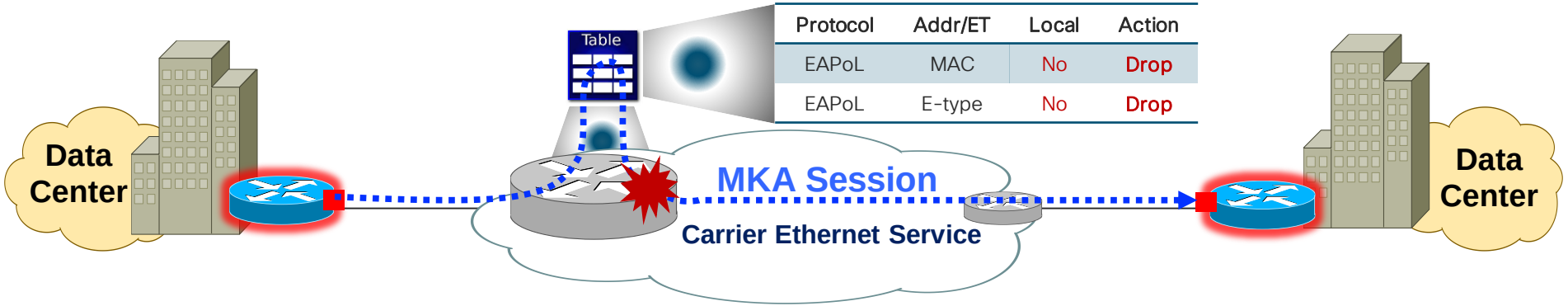


Ethernet Frame

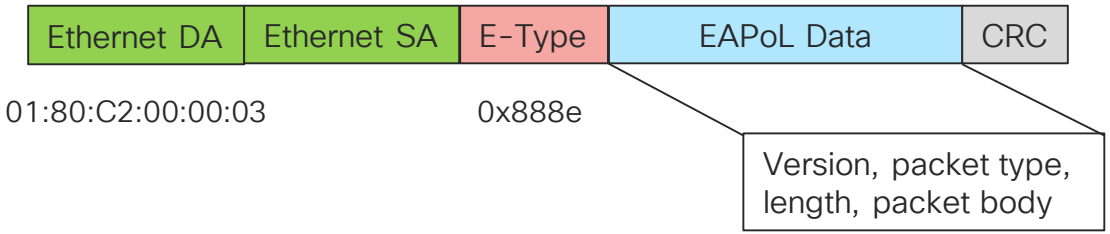


- Provider bridge may be programmed to injest and inspect elements of the EAPoL frame (destination address and/or ether-type)

WAN MACsec Use Cases
High Speed Site to Site



Ethernet Frame



- Provider bridge, if EAPoL is NOT destined for use, will DROP the frame mid-stream of the EAPoL session between two MACsec stations

EAPoL “Destination Address” Change Command

- The “eapol destination-address” command allows the operator to change the destination MAC address of an EAPoL frame
- This ensures EAPoL frame is “unknown” to service provider bridge

CLI Example (IOS-XE):

```
...
interface GigabitEthernet0/0/4
  macsec dot1q-in-clear 1*
  macsec replay-protection-window-size 100
  eapol destination-address broadcast
```

Leverage “broadcast” address as the destination EAPoL address. Provider switch will forward as standard “broadcast” Ethernet frame.

EAPoL “Ether Type” Change Command

- The “macsec eth-type” command allows the operator to change the destination Ether Type value of an EAPoL frame
- This ensures EAPoL ether-type is “unknown” to service provider bridge

CLI Example (IOS-XE)

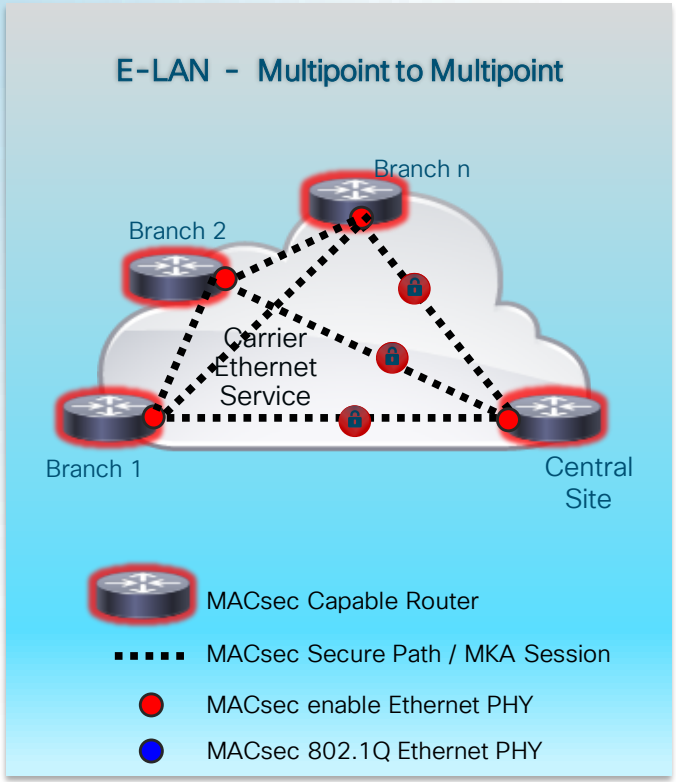
```
...
interface GigabitEthernet0/0/4
  macsec dot1q-in-clear 1*
  macsec replay-protection-window-size 100
  eapol destination-address broadcast
  eapol eth-type 876F
```

Leverages a “well known” ether type value.

Provider bridge will NOT ingest frame as ether-type 0x876F as it is assumed “well known”.

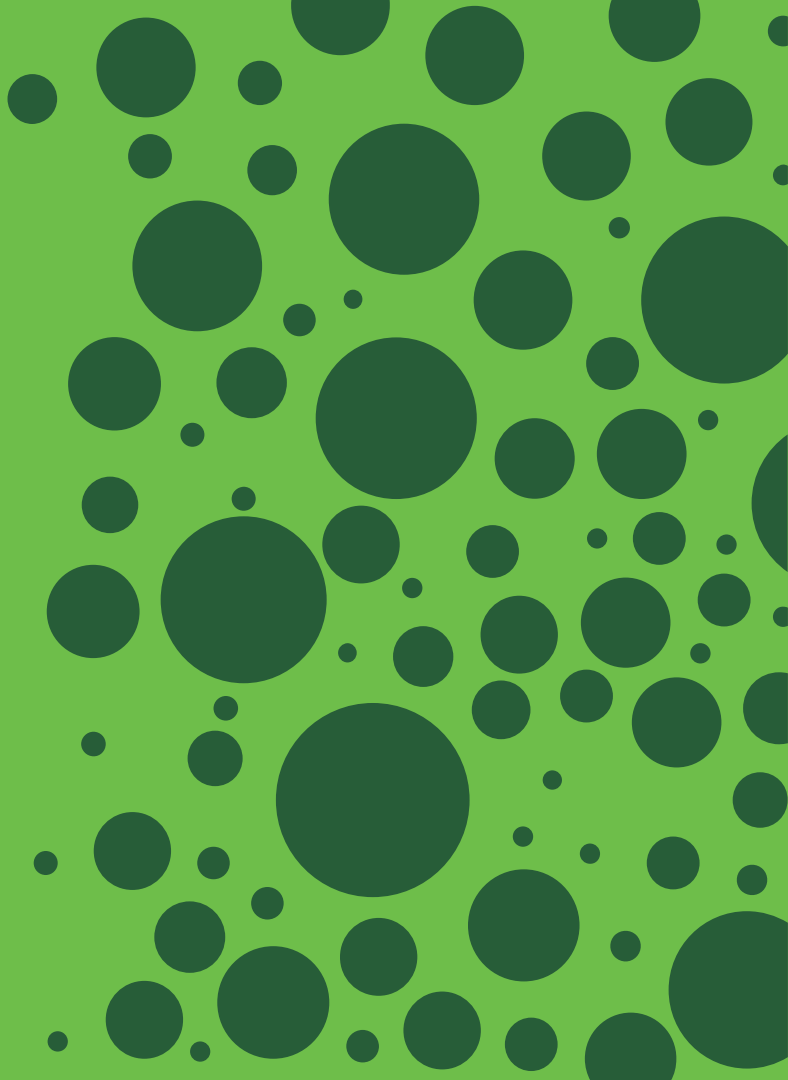
WAN MACsec Use Cases
Point to Multi-point / Multi-point to Multi-point Topology

- Use Case - Requirement
  - High Speed Any-to-Any Topology Support
    - Targets ~30 sites (10G PHY), 64 SA HW limit
  - Traffic patterns dictated by business application behavior
- WAN MACsec Features
  - Leverage 802.1Q in the clear (Hub-Site logical separation)
  - Leverage (if needed) use of EAPoL "destination-address" and "ether type change control feature
- Key Benefits
  - Simple to configure
  - Ability for router to adjust to providers Ethernet services
  - 802.1Q Tag in Clear allows simple site aggregation



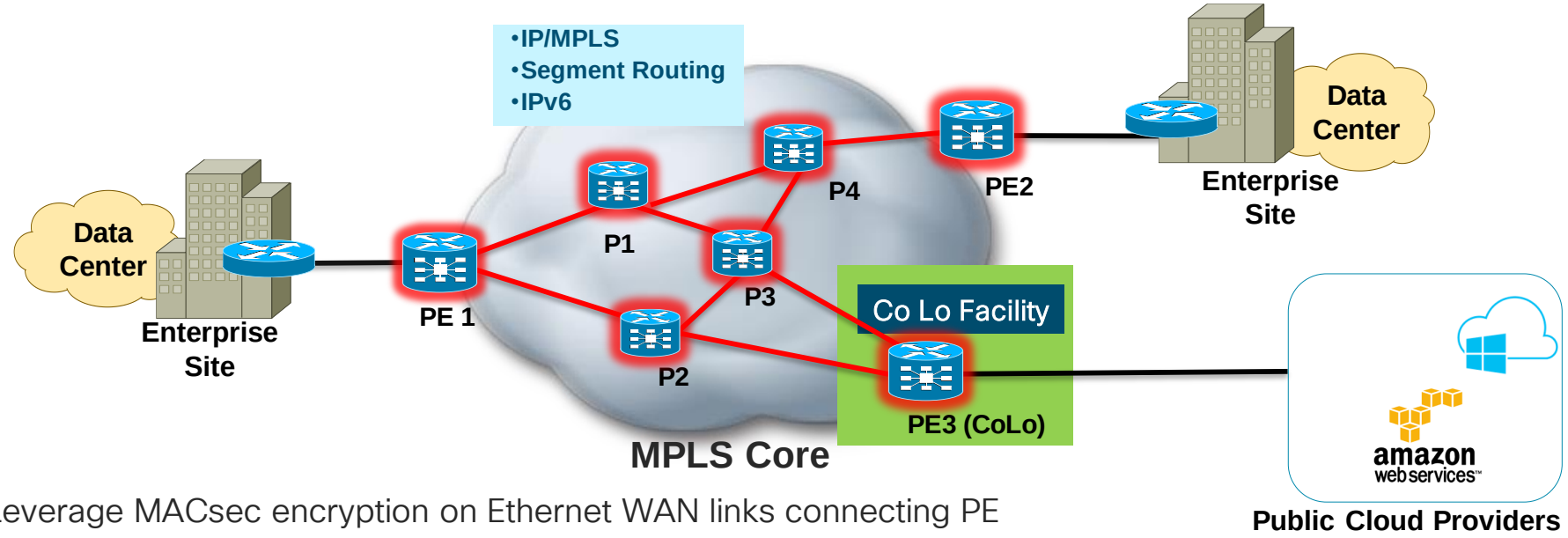
Use Cases

Securing Private IP / MPLS / Segment Routing Backbone



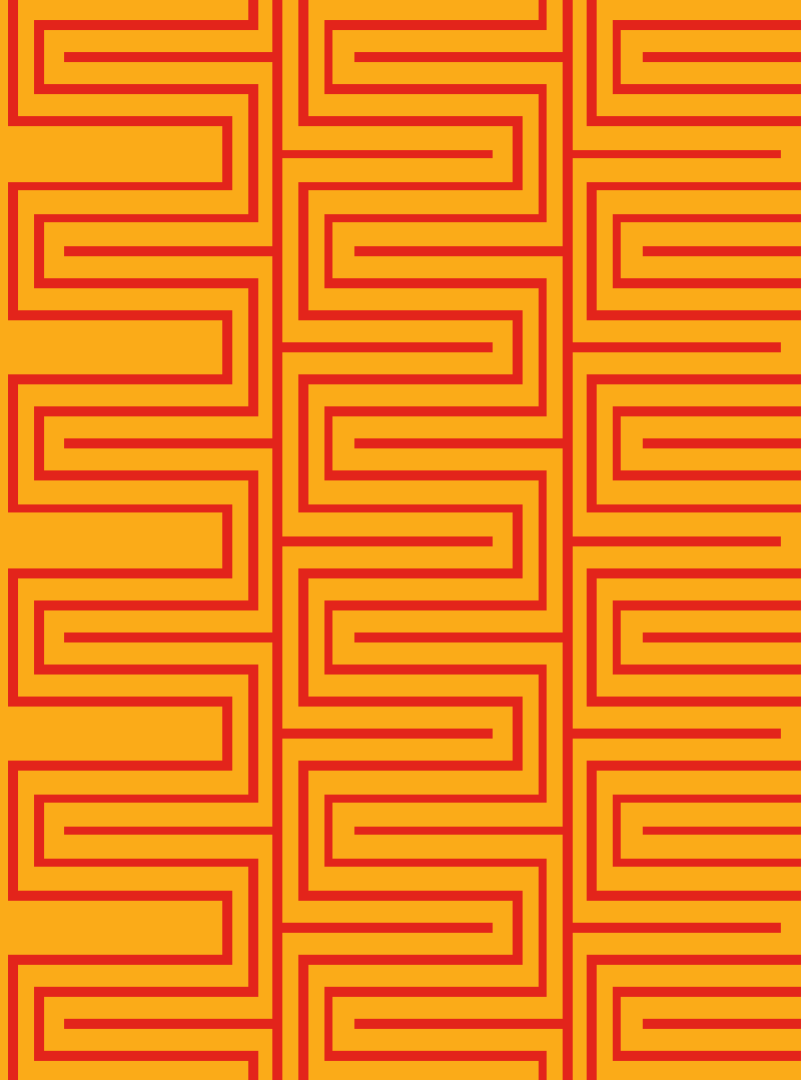
WAN MACsec for Secure MPLS Backbone

Per Link Encryption at 100Gb+ with MACsec End-to-End

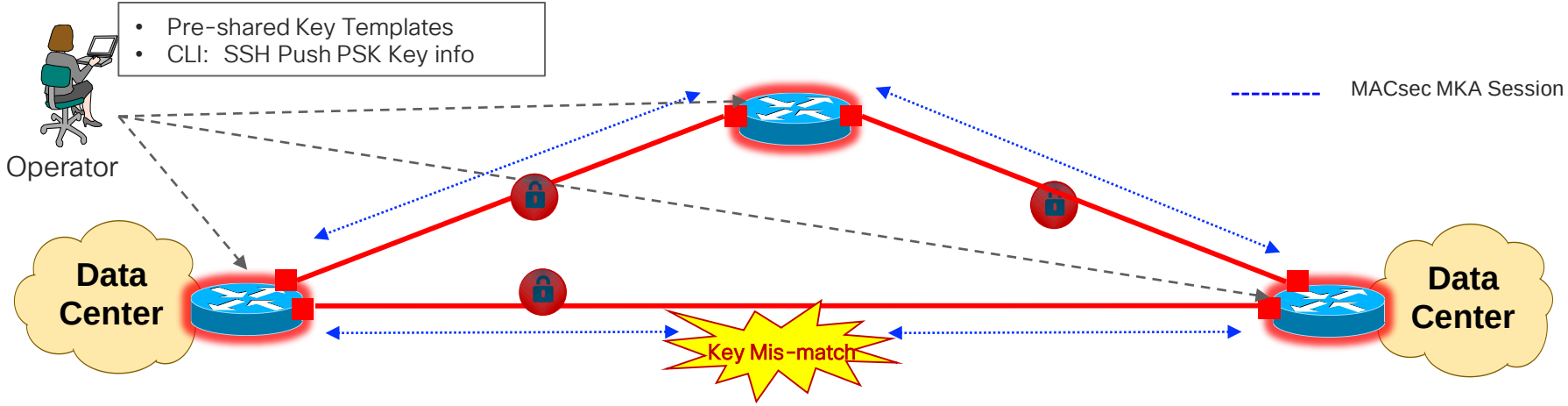


- Leverage MACsec encryption on Ethernet WAN links connecting PE and P routers in MPLS Core (up to 100GE, N x 100GE)
- Offers “per hop” encryption and telemetry at each PE / P router
- Transparent to MPLS/Segment Routing, TE, multicast (e.g. No GRE Needed!!! ☺)
- Ideal solution for extending private backbone to CoLo (e.g. Equinix)

High Availability Use Case for WAN MACsec Designs



MACsec Configuration Recommendation
Implement Bi-Directional Forward Detection (per link)

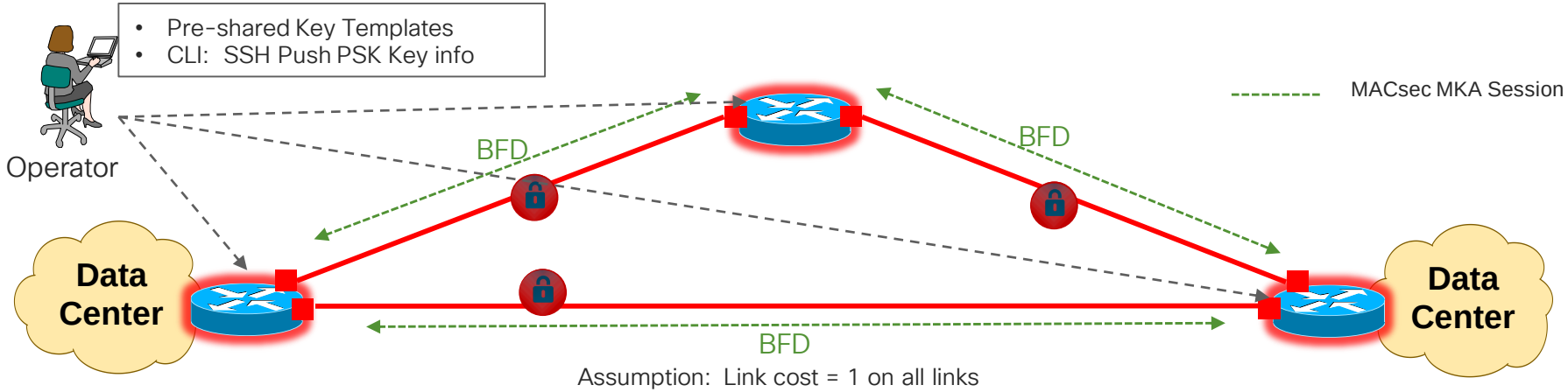


Challenges:

- Updating Pre Shared Keys (PSK) is a manual process
- Opens possibility of mistakes during process (mis-types, comm loss)
- MKA keepalive intervals are much longer than IGP or BFD timers
- Mis-configured MACsec keys, cause a black-holing affect on traffic

Assumption: Link cost = 1 on all links

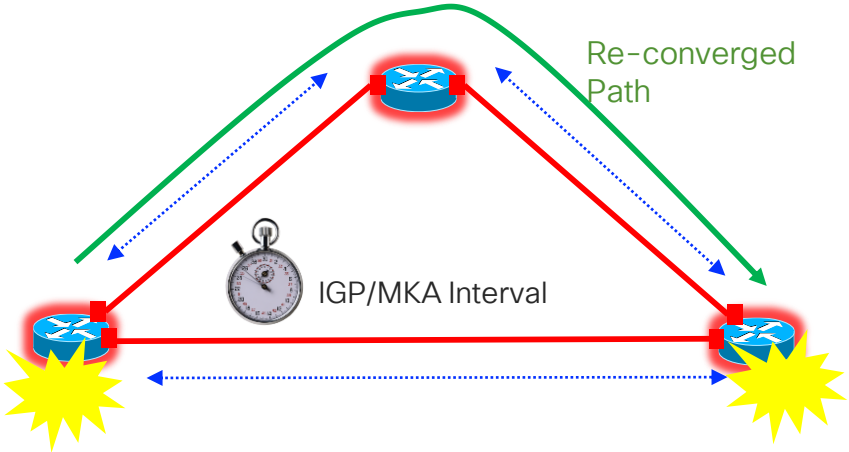
MACsec Configuration Recommendation
Convergence Impacts Around MACsec Key Operations



- Solution: Network configurations should include the prevention of black-holing traffic in the event there is a mis-configuration of PSK changes on a router
- Apply Bi-Directional Forward Detection (BFD) to WAN Ethernet Links running MACsec

MACsec Configuration Recommendation
Inject BFD for Traffic Convergence Around MACsec Failures

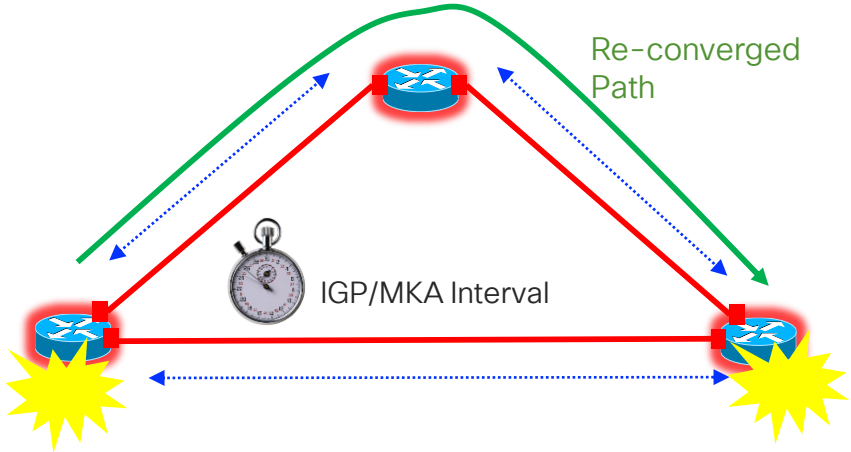
10's of Seconds using IGP/MKA Timers



- Mis-configured keys or MACsec failures dependent on IGP or MKA time-out to converge
- Convergence in 10's of seconds

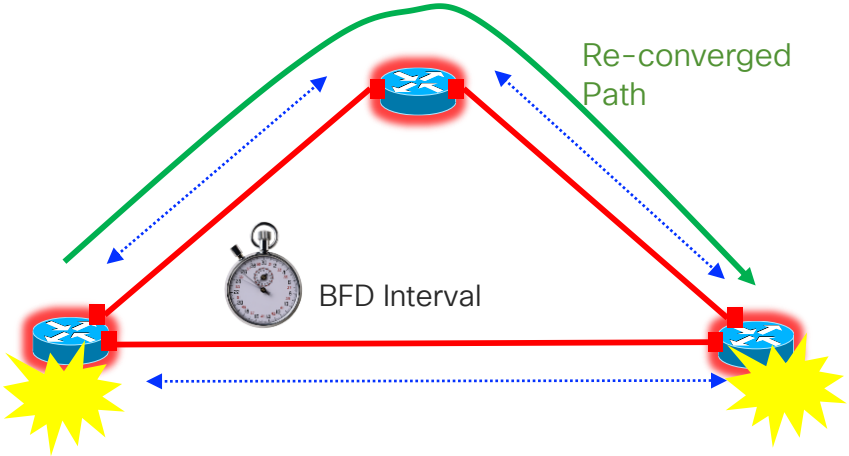
MACsec Configuration Recommendation
Inject BFD for Traffic Convergence Around MACsec Failures

10's of Seconds using IGP/MKA Timers



- Mis-configured keys or MACsec failures dependent on IGP or MKA time-out to converge
- Convergence in 10's of seconds

Sub-second Convergence using BFD

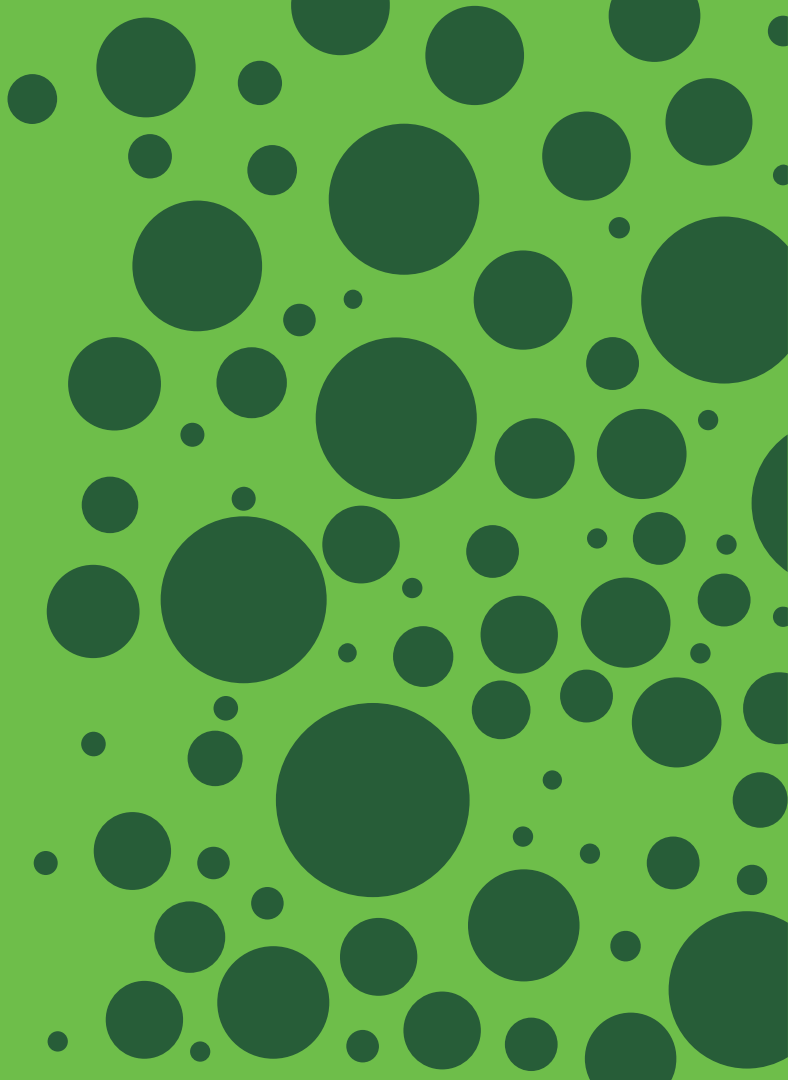


- Mis-configured keys or MACsec failures will trigger BFD process
- Offer sub-second convergence and protection

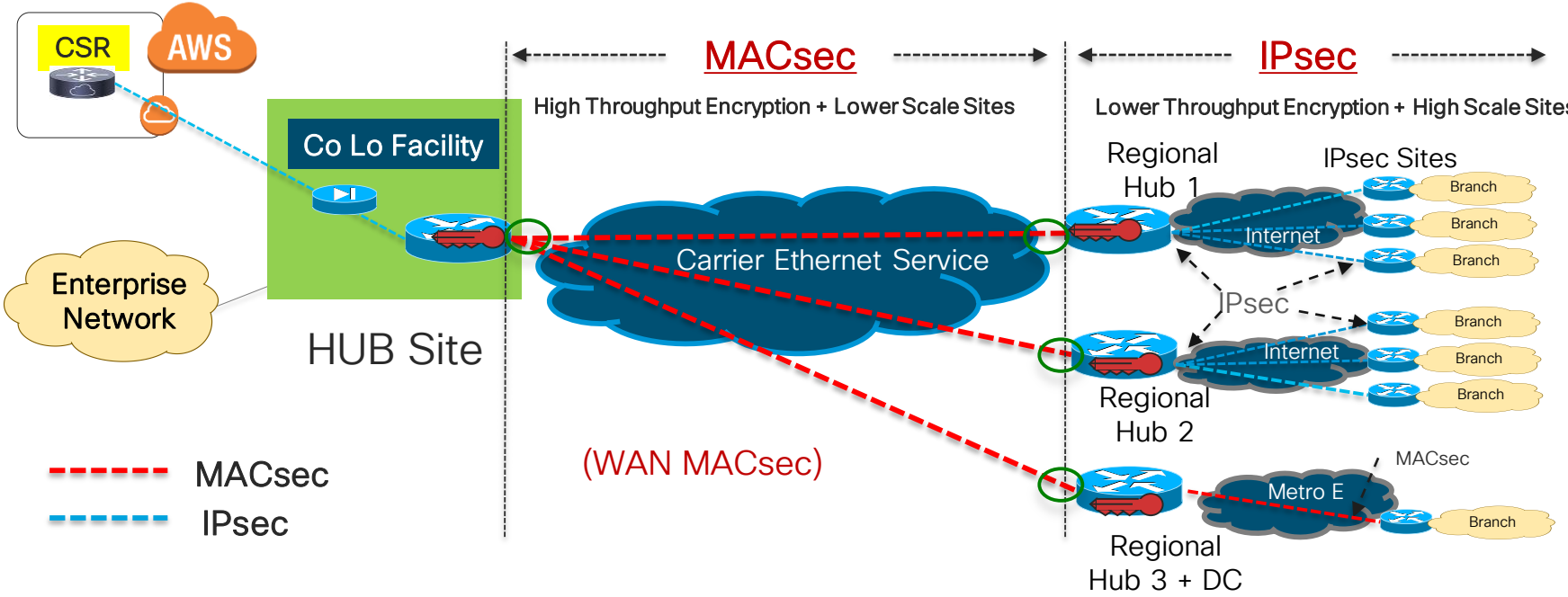
Use Cases

Hybrid WAN Encryption Design

WAN MACsec + IPSec

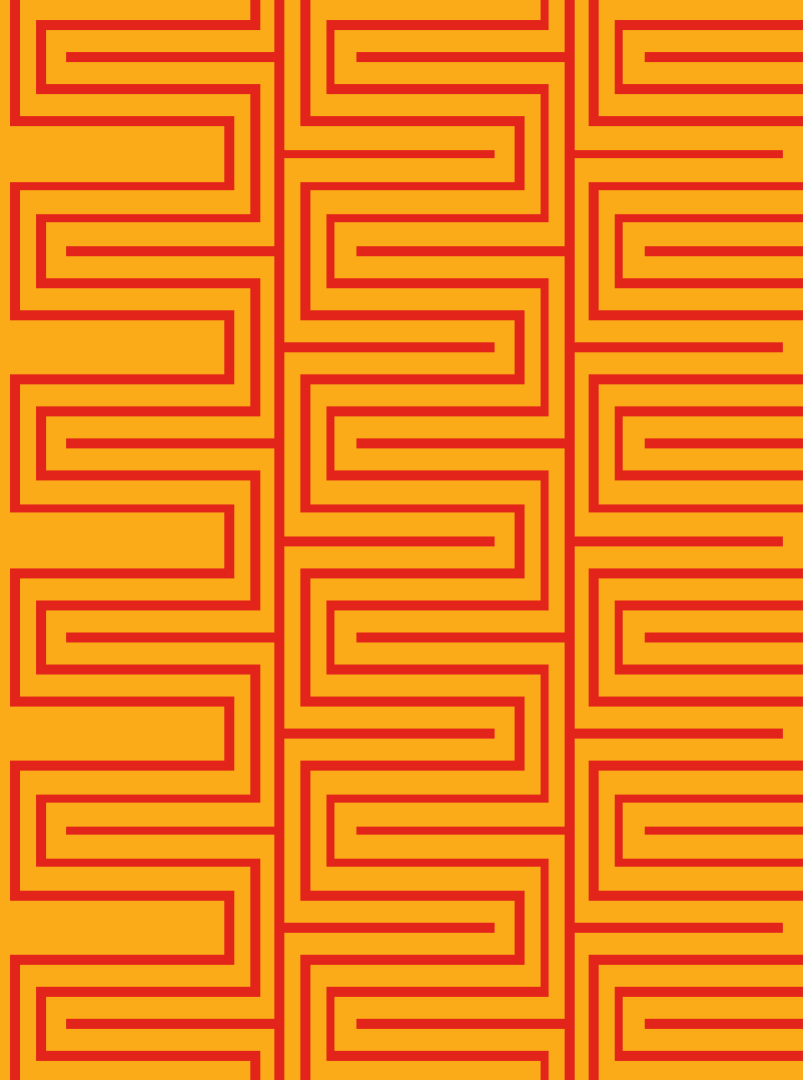


Hierarchical “Hybrid” MACsec + IPSec Design

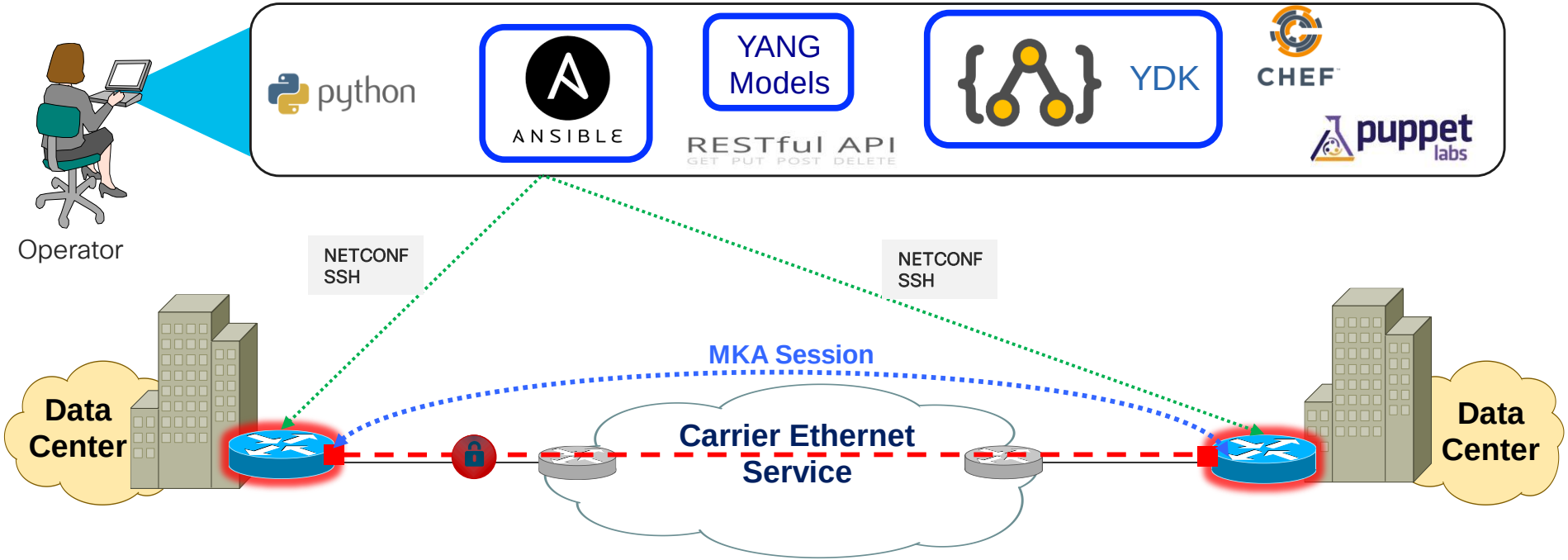


- “Hybrid” design option for mix of scale, performance, leveraging Ethernet services
- MACsec: Backbone/Core – Targets Higher BW, Lower Number of Sites
- IPSec: Branch/back-haul – Targets Lower BW, high number of sites, cloud (CSR)

Adding Automation to Security Operations



WAN MACsec Operations
Automating WAN MACsec Pre-Shared Key (PSK) Changes



- Leverage open source automation tools to speed up operations

MACsec Tasks That Could Leverage Automation

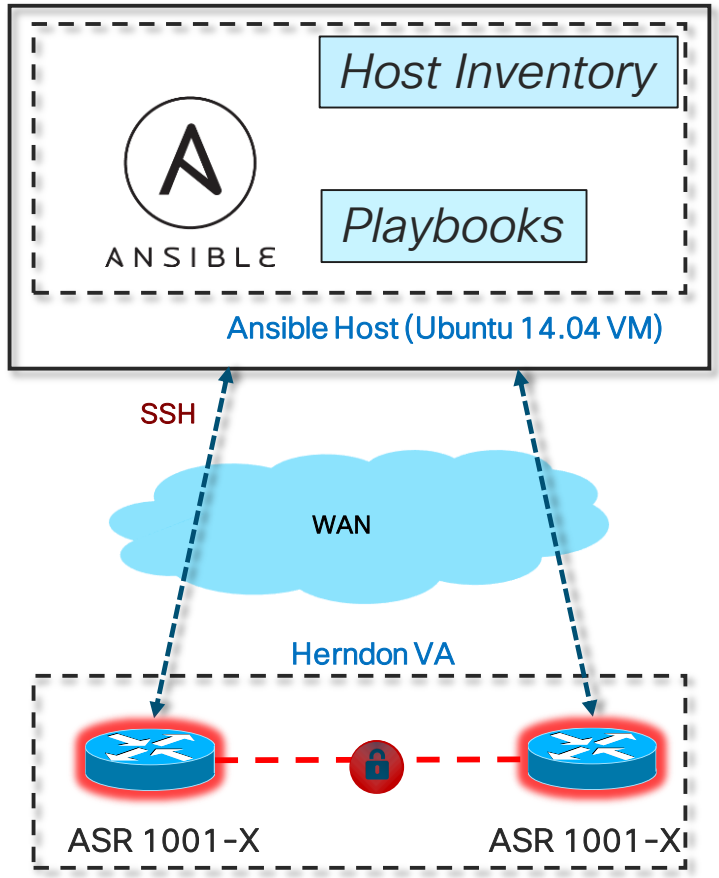
- Creating a MACsec Key Chain
  - Chain, key string, key lifetime
- Creating a User-Defined MACsec Policy
  - Cipher, confidentiality offset, priority
- Applying MACsec Configuration on an Interface
- Verifying MACsec Encryption enabled
  - Assure policy enabled, secure peering, cipher's used

Target those operations tasks that are repeatable, requires touching on all security devices, and are often a burden to the Sec/NetOps teams

Ansible for NetOps
Automating MACsec Key Chain Changes

- Ansible 2.2.1 (Linux VM)
- Cisco ASR 1001-X (XE 16.3.2)

- Playbook:
  - SSH credential
  - key chain name: June-key
  - Key number: 01
  - cryptographic-algorithm aes-128-cmac
  - key-string: 1234567890..... 23456789011
  - Lifetime: 00:00:00 Jun 1 2017 23:59:59 Jun 30 2017



GitHub Repository to Example:
https://git.io/vQUR3

Yang Models for MACsec

Yang Model Support for MACsec – IOS-XR

Source: https://github.com/YangModels/yang/tree/master/vendor/cisco/xr/621

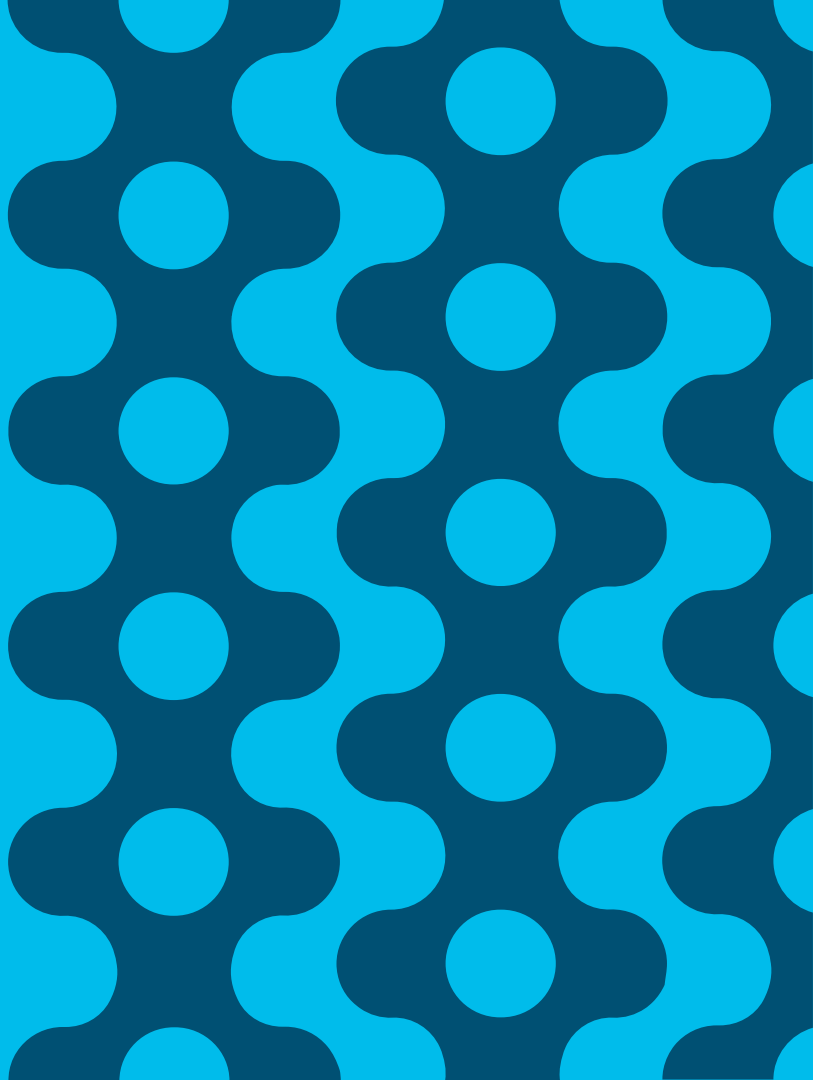
- Cisco-IOS-XR-crypto-macsec-mka-cfg.yang
- Cisco-IOS-XR-crypto-macsec-mka-if-cfg.yang
- Cisco-IOS-XR-crypto-macsec-mka-oper-sub1.yang
- Cisco-IOS-XR-crypto-macsec-mka-oper.yang
- Cisco-IOS-XR-crypto-macsec-secy-oper-sub1.yang
- Cisco-IOS-XR-crypto-macsec-secy-oper.yang
- Cisco-IOS-XR-lib-keychain-macsec-cfg.yang
- Cisco-IOS-XR-macsec-ctrlr-oper-sub1.yang
- Cisco-IOS-XR-macsec-ctrlr-oper.yang
- Cisco-IOS-XR-ncs1k-macsec-ea-oper-sub1.yang
- Cisco-IOS-XR-ncs1k-macsec-ea-oper.yang

External Resources (GitHub)

https://github.com/netwrkr95

- **Ansible – MACsec Keychain Examples**
  - Ansible WAN MACsec Playbook and Configs (https://git.io/vQUR3)
- **YANG Models – MACsec Keychain Examples (Using YDK)**
  - MACsec Key Chain Configuration applications (https://git.io/vH7uD)
  - What is YDK? (https://developer.cisco.com/site/ydk/)
- **Ansible Module Using YANG Models with YDK**
  - Ansible + YDK app (https://git.io/vH7XZ)

Solution Roadmap



(Subject to change)

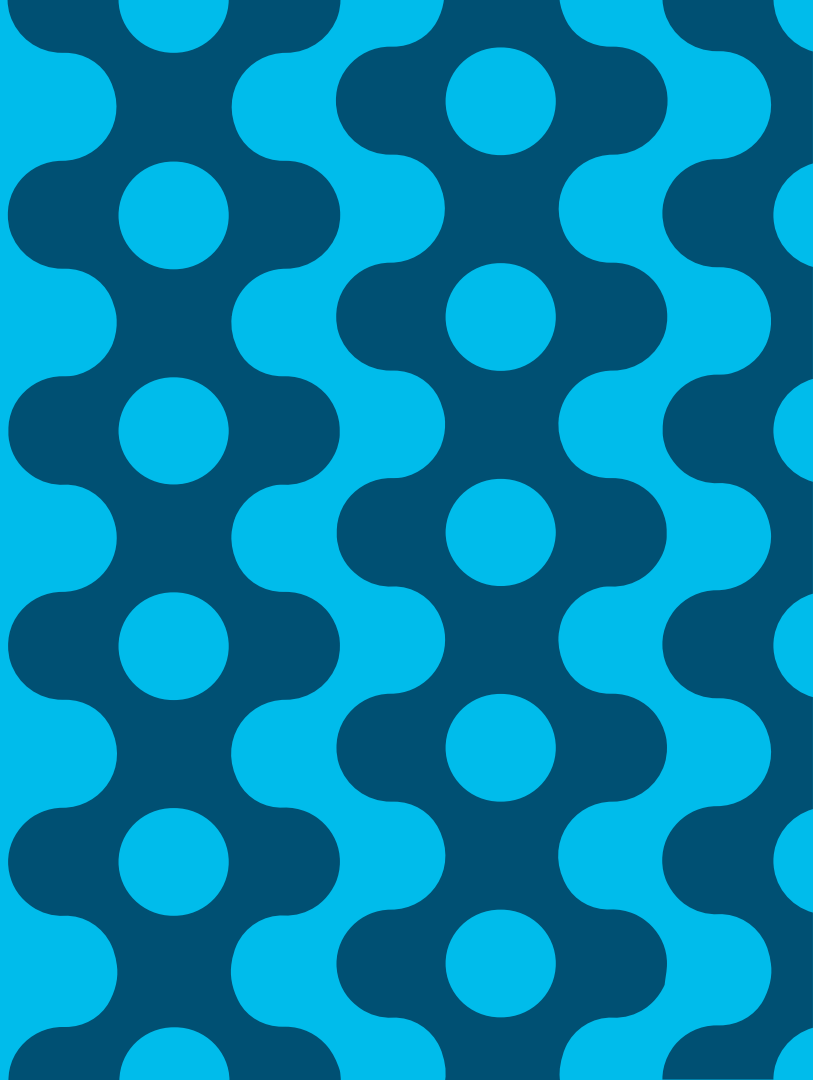
Cisco MACsec Portfolio (Summarized Version)

Platform Series	MACsec Delivery	MACsec Speed (AES-256)
ISR 1K/4K Series	• 1p/2p Ether NIM, fixed (on 1K)	• 1GE
ASR 1000 Series	• Fixed and Modular solutions	• 1GE, 10GE
ASR 9xxx Series	• Modular Line Cards	• 1GE*, 10GE, 40GE, 100GE
NCS 55xx Series	• Modular and Fixed (QSFP ports)	• 100GE (QSFP only)
Nexus 7700 Series **	• Modular M3 Series Card	• 1/10GE, 40GE, 100GE
Nexus 9000 Series	• Fixed and Modular solutions	• 10GE, 40GE, 100GE
Optical NCS Series	• NCS2k, NCS4k, Client ports	• 10GE, 40GE, 100GE
Catalyst Switching	• C3650, C3850, C9xxx	• 1GE, 10GE, 40GE
Catalyst Switching **	• Cat 4K, 6K	• 1GE, 10GE

** Currently does NOT support MKA key negotiation (SAP only)

Cisco Account Teams can provide more details

Putting it All Together – Positioning, Use Cases



Positioning the Proper Encryption Solution

- It is important NOT to position encryption solutions against one another
- Rather, consider each as a tool in the tool bag, which requires a positioning exercise to meet the technical and business req
- Key Factors for encryption decisions will include:
  - Transport availability / options
  - Performance requirements of the solution/application
  - Scale of the design and requirements (number of spokes, connected end-points, aggregate encryption)
- Beyond IPSec, “the underlying transport dictates the available encryption options that can be leveraged”

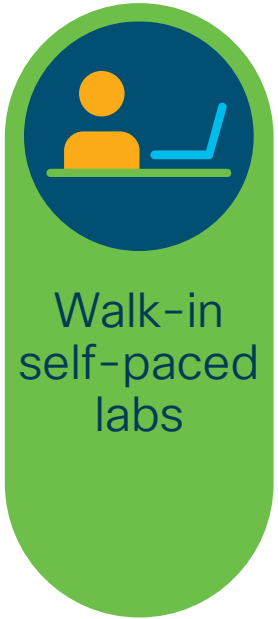
Complete your online session evaluation

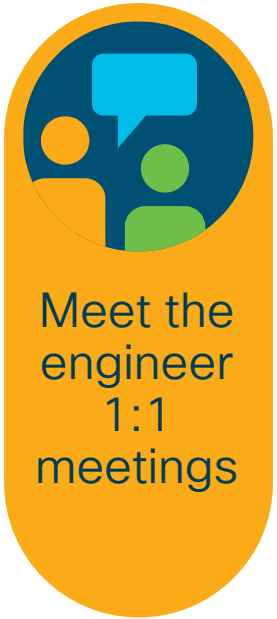
Give us your feedback to be entered into a Daily Survey Drawing.

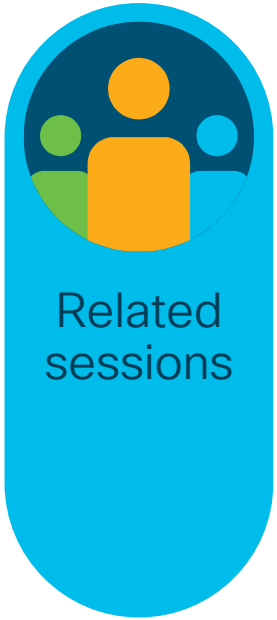
Complete your session surveys through the Cisco Live mobile app or on www.CiscoLive.com/us.

Don't forget: Cisco Live sessions will be available for viewing on demand after the event at www.CiscoLive.com/Online.

Continue your education







Thank you