Corso di QoS e Sicurezza nelle reti

Il protocollo IPv6

(29-04-2015)

Ing. Peppino Fazio

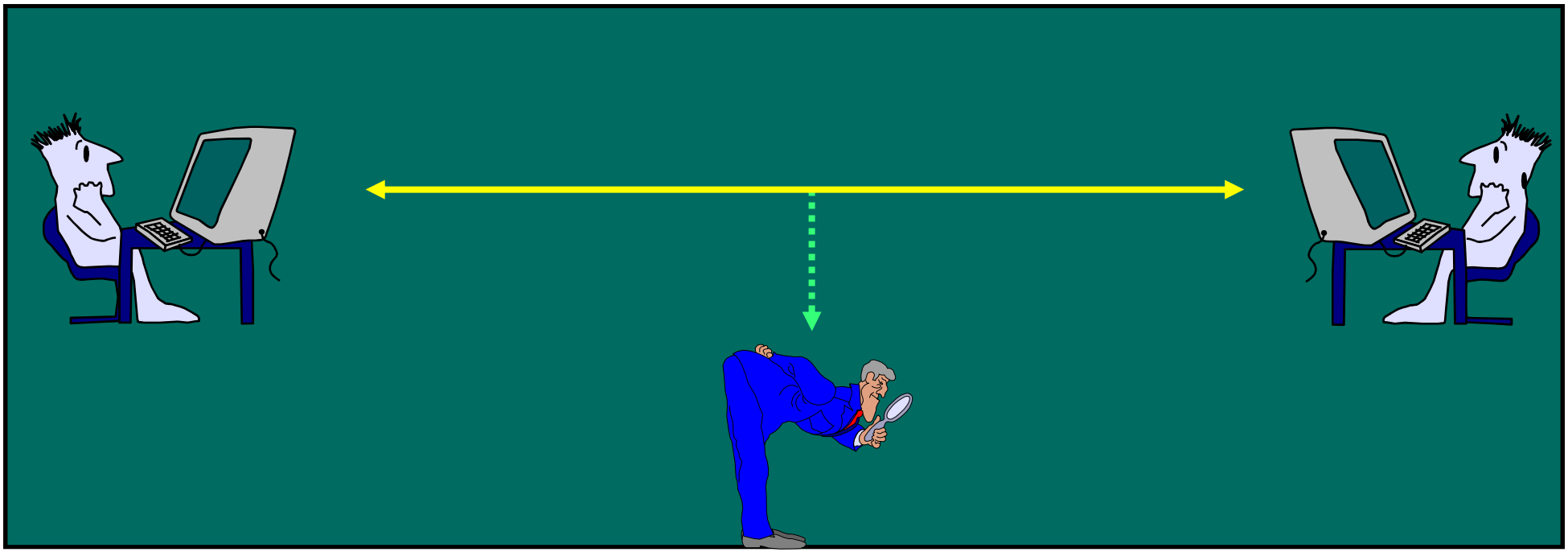
A.A. 2014/2015

IPv6 Security

- Implementare meccanismi di security a livello IP garantisce un networking "sicuro" a tutti i tipi di applicazioni (sia a quelle che hanno meccanismi di security propri sia a quelle che non ne hanno)
- La sicurezza a livello IP include 2 aree: autenticazione (integrità) e confidenzialità (privacy) dei dati
- Il meccanismo di autenticazione dei dati dà assicurazione sulla identità della sorgente e inoltre garantisce che il pacchetto in transito non venga alterato (integrità)
- La confidenzialità dei dati assicura che questi non vengano usati da altri se non il destinatario; si usano tecniche di crittografia

Crittografia

- Consiste nell'alterazione controllata di un messaggio (sequenza alfanumerica di caratteri) in maniera da renderlo non leggibile a chi non dispone degli strumenti adeguati



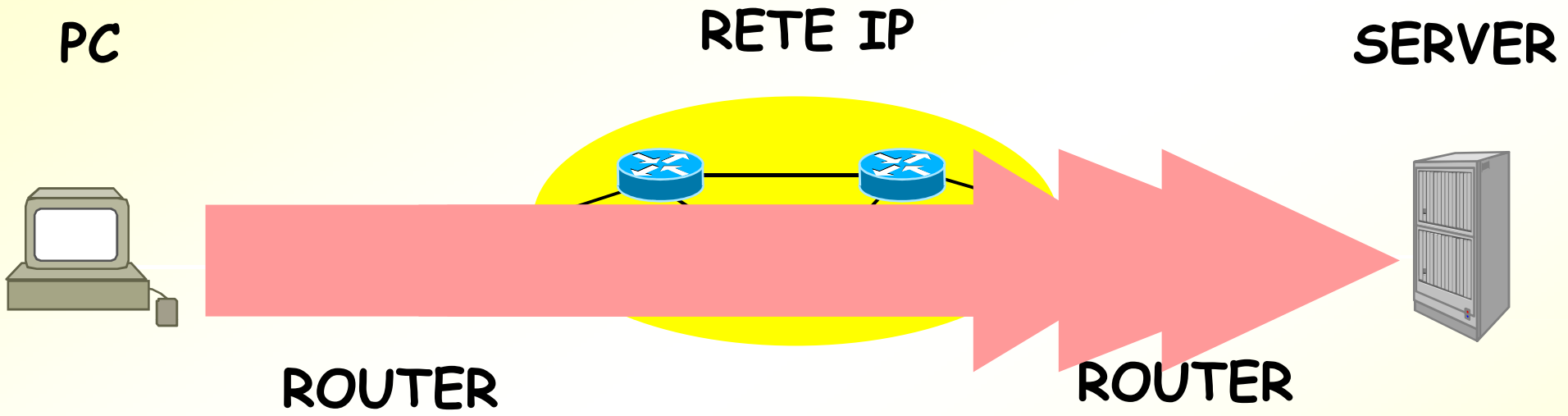
IPv6 Security

- Le tecniche di IP security (IPSec) sono state specificate negli RFC 1825-1829; la versione ultima è l'RFC 2401 (1998);
- In entrambi i casi, le caratteristiche di sicurezza sono implementate come extension header
- L'extension header usato per l'autenticazione è detto Authentication header (AH); quello usato per la privacy è l'Encapsulating Security Payload (ESP) header

IPv6 Security

- **Integrity:** assicura che le modifiche ai dati siano rilevabili
- **Data Origin Authentication:** verifica l'identità della sorgente dei dati
- **Confidentiality:** è il servizio di sicurezza che protegge i dati da accessi non autorizzati
- **Encryption:** è un meccanismo di sicurezza usato per trasformare i dati da una forma intelligibile (plaintext) in una non intelligibile (ciphertext), per fornire la confidenzialità.
- **Access Control:** è un servizio di sicurezza che impedisce l'uso non autorizzato di una risorsa

Utilizzazione di AH e ESP



- AH ed ESP possono essere impiegati per stabilire comunicazioni "sicure" tra PC e Server, tra Router e server o tra Router

Firewall

- Il termine firewall identifica in modo generico una serie di funzioni e di apparecchiature che servono a proteggere un determinato dominio o rete privata
- Più specificamente, si intende per firewall un insieme di componenti che interconnettono due reti e che possiedono le seguenti proprietà:
  - tutto il traffico di dati entrante ed uscente dalla rete interna e viceversa deve passare attraverso il firewall
  - solo il traffico autorizzato può passare attraverso il firewall
  - il firewall è immune (o almeno si spera) da accessi illegali

Firewall

- Uno dei componenti fondamentali del firewall e il security gateway (o screening router)
- Può essere un router commerciale o un router basato su un host
- La caratteristica principale è la capacità di filtrare i pacchetti IP in base all'indirizzo di sorgente e di destinazione, permettendo il passaggio dei dati solo se vengono rispettate determinate associazioni tra gli indirizzi sorgente e destinazione

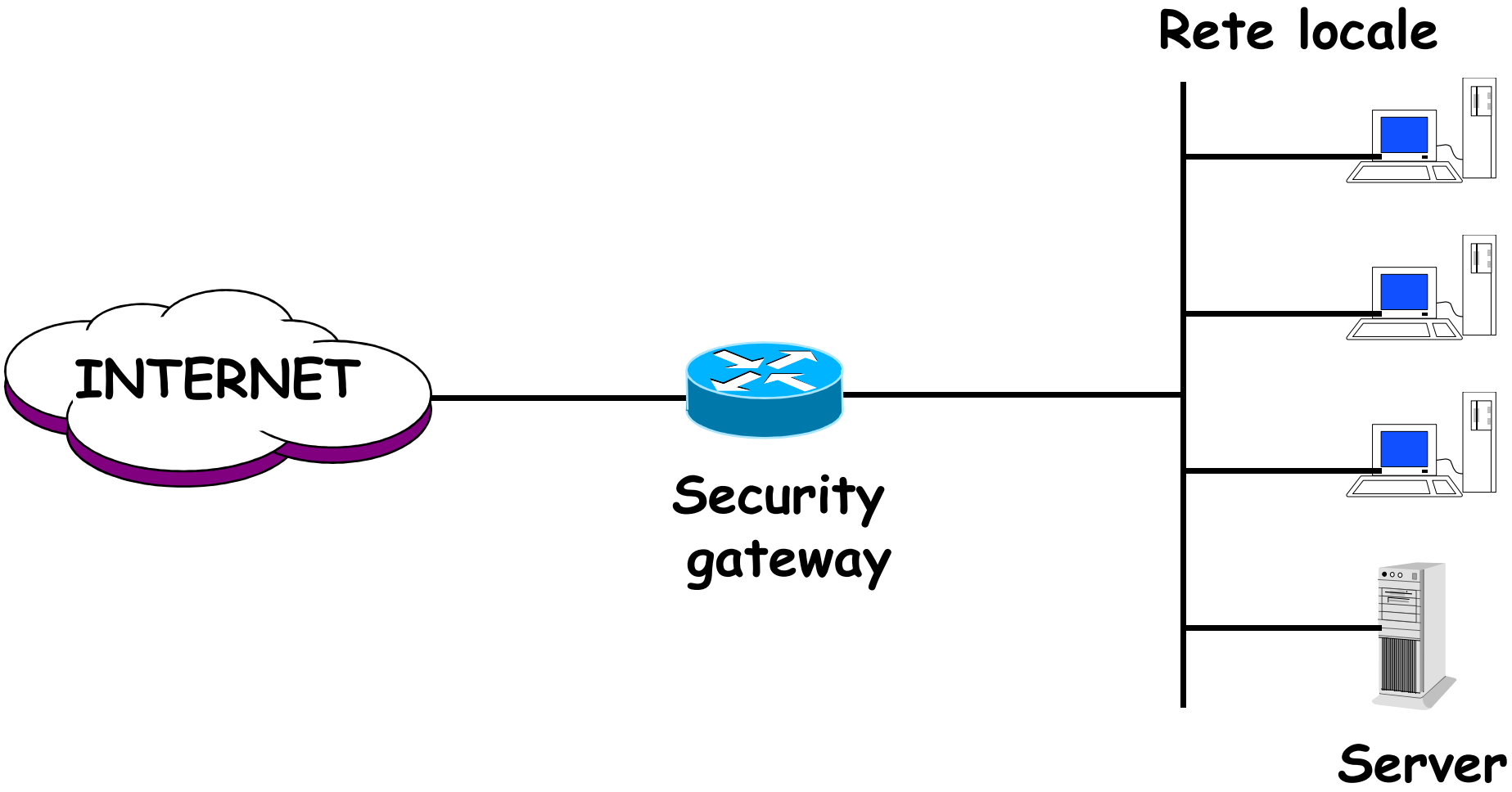
Security Gateway

Security Gateway (SG)

è un sistema intermedio che agisce da interfaccia di comunicazione tra due reti. La rete esterna è considerata "untrusted", mentre reti e host interni sono considerati "trusted". In IPsec, un SG è un punto in cui è implementato AH e/o ESP per servire un set di host interni, fornendo servizi di sicurezza quando essi comunicano con host esterni che usano anche IPsec (direttamente o tramite un altro security gateway).

- Trusted Subnetwork: contiene host e router che "si fidano" l'uno dell'altro e si impegnano a non effettuare attacchi attivi o passivi. Si assume anche che il canale di comunicazione (e.g., LAN) non sia attaccabile con altri mezzi.

Security Gateway



Security Association (SA)

- E' un concetto di base per l'IP security
- Le Associazioni di Sicurezza identificano univocamente tutti i parametri necessari per una comunicazione sicura fra due parti (ad es. algoritmo di cifratura, modalità, chiavi, funzioni hash)
- Una Security Association (SA) è una "connessione" logica, a livello IP a una via (simplex) tra un nodo trasmettitore e un ricevitore, che garantisce servizi di sicurezza al traffico che viene da essa trasportato
  - Tutto il traffico trasportato su una SA è fornito degli stessi meccanismi di protezione e sicurezza
- Per avere uno scambio di traffico "sicuro" bidirezionale, allora servono due SA
- Ogni SA si riferisce a un particolare protocollo (AH o ESP); per applicare al traffico entrambi i tipi di protezione (AH e ESP) bisogna definire 2 (o più) SA

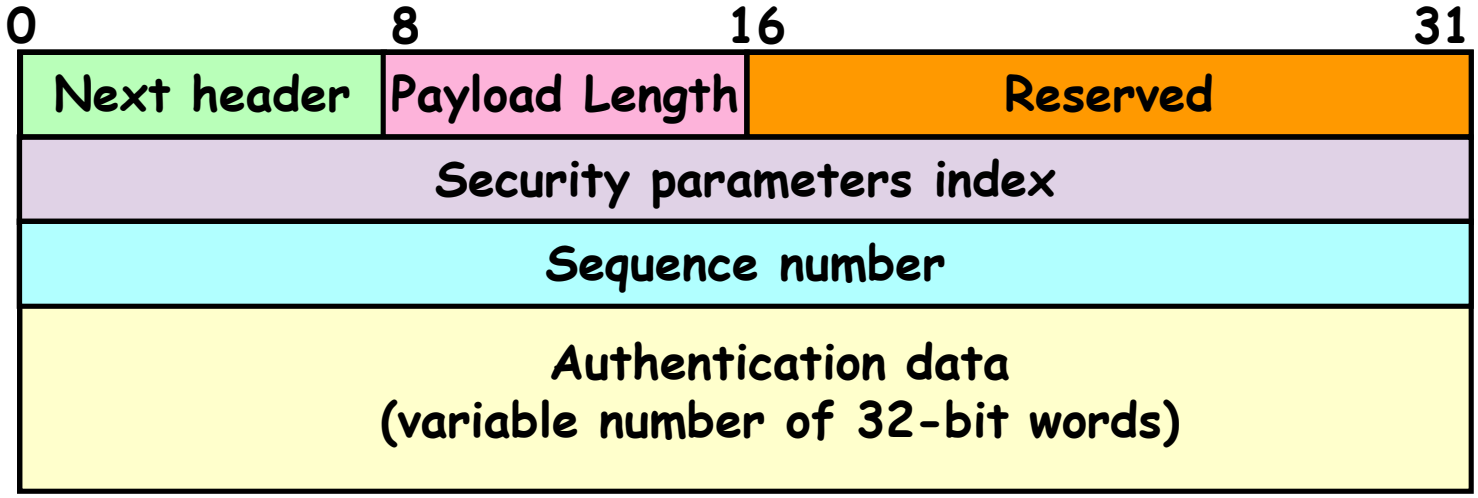
Security Association

- Parametri che caratterizzano una Security Association
  - Algoritmo di Autenticazione e chiave(i) per l'AH (necessario)
  - Algoritmo di encryption e chiave(i) per l'ESP (necessario); l'algoritmo di default è il Message Digest 5 (MD5)
  - Presenza/assenza e dimensione di un campo di sincronizzazione crittografica o "initialization vector", per l'algoritmo di encryption (necessario)
  - Algoritmo di Autenticazione e chiave(i) per l'ESP (raccomandato)
  - Tempo di vita per la chiave(i) o istante in cui la chiave(i) deve cambiare (raccomandato)
  - Tempo di vita della Security Association (raccomandato)
  - Indirizzo(i) di sorgente della Security Association (raccomandato)
  - Sensitivity level (secret o unclassified), cioè il tipo di protezione per i dati (necessaro o raccomandato)

Authentication header (RFC 2402)

- L'Authentication Header (AH) fornisce l'integrità dei dati e l'autenticazione della sorgente dei pacchetti IP
- Il calcolo dell'autenticazione è effettuato prima della eventuale frammentazione dalla sorgente e dopo lo eventuale riassemblamento dalla destinazione
- Le informazioni di autenticazione sono calcolate utilizzando tutti i campi del datagramma IP che non cambiano durante il trasporto
  - i campi che variano nel transito sono settati a 0 nel calcolo dell'algoritmo di autenticazione sia alla sorgente che alla destinazione
  - per IPv6 i campi variabili sono Hop limit, alcuni campi option type negli extension header Hop-by-hop options e Destination options

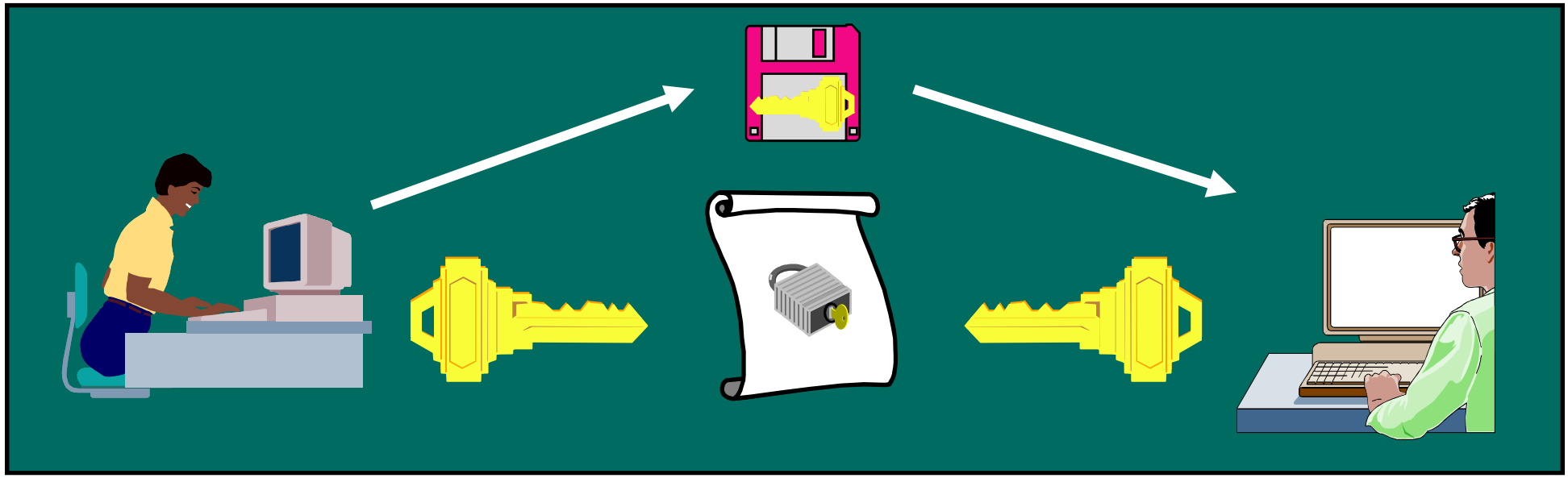
Authentication header



- Next header (8 bit): identifica il tipo di header successivo
- Payload Length (8 bit): lunghezza dell'AH, in unità di 4 byte, meno 2
- Reserved (16 bit): per usi futuri (settato a 0)
- Security parameters index (SPI) (32 bit): valore arbitrario assegnato dal sistema di destinazione, identifica, con destination IP address e security protocol (AH), la security association per il datagramma
- Sequence number (32 bit): è un contatore inizializzato a 0 quando la SA viene attivata e incrementato in ogni datagramma
- Authentication data (variable): il contenuto dipende dall'algoritmo di autenticazione usato per il calcolo dell'Integrity Check Value (ICV)(in RFC1828 l'algoritmo MD5 usa 16 byte)

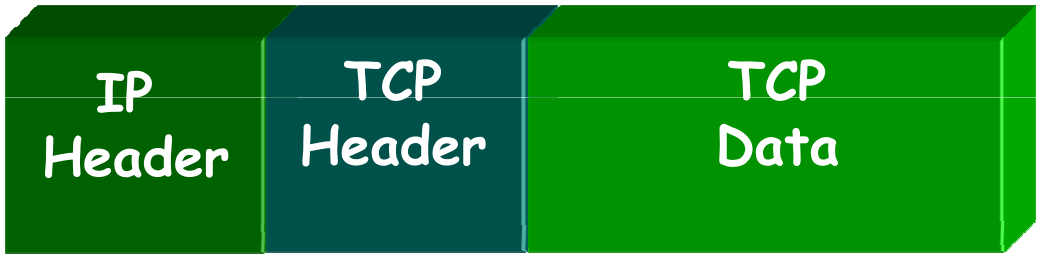
Authentication header

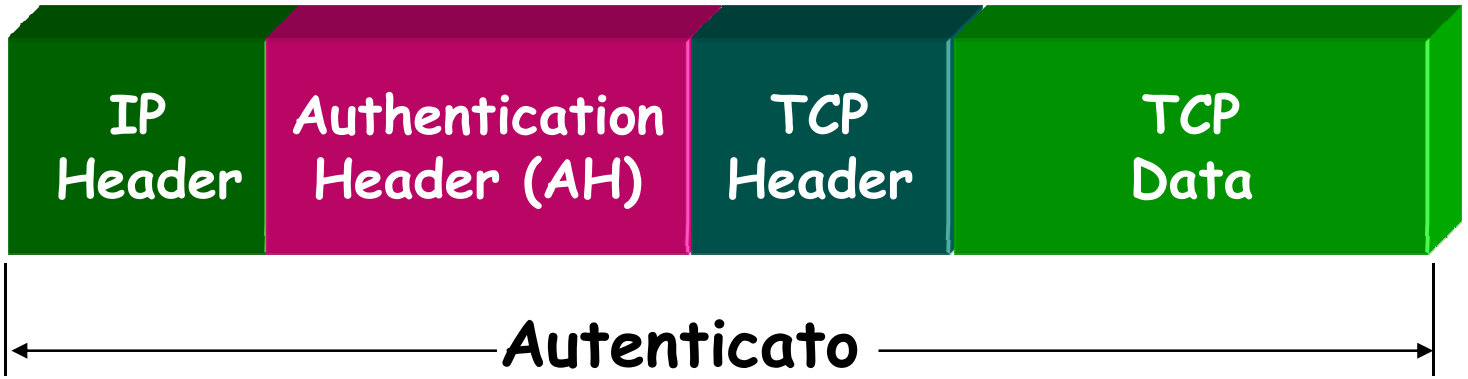
- I 128 bit del campo Authentication data sono calcolati dall'algoritmo MD5 sulla base di
  - i bit del datagramma
  - la chiave segreta di encryption del sender
- il ricevente verifica l'autenticità del datagramma compiendo l'operazione inversa mediante la stessa chiave



Authentication Header: Transport Mode

- La modalità "Transport" (esiste anche la modalità tunnel) protegge il segmento a livello di trasporto
  più campi selezionati dell'header IP (quelli non variabili)
- E' usata nelle implementazioni per gli host





L'indirizzamento IPv6

RFC 2373

Indirizzi IPv6

- IPv6 usa indirizzi di 128 bit
- Gli indirizzi sono assegnati alle singole interfacce o a gruppi di interfacce sui nodi e NON ai nodi stessi (host/router)
- IPv6 specifica 3 tipi di indirizzi: unicast, anycast e multicast
- Non esiste più l'indirizzamento broadcast; le sue funzioni sono sostituite dall'indirizzamento multicast

Indirizzi IPv6

- **Unicast**: un identificatore per ogni interfaccia
  - un pacchetto inviato a un indirizzo unicast viene consegnato all'interfaccia specificata dall'indirizzo
- **Anycast**: un identificatore per un set di interfacce (tipicamente di nodi diversi)
  - un pacchetto inviato a un indirizzo anycast viene consegnato a una delle interfacce specificate dall'indirizzo (la più vicina, in base alla metrica di routing usata)
- **Multicast**: un identificatore per un set di interfacce (tipicamente di nodi diversi)
  - un pacchetto inviato a un indirizzo multicast viene consegnato a tutte le interfacce specificate dall'indirizzo

Indirizzi IPv6

- Un indirizzo IPv6 unicast si riferisce a una sola interfaccia
  - dato che ogni interfaccia appartiene ad un nodo, ciascuno degli indirizzi unicast delle sue interfacce può essere usato per individuare univocamente quel nodo
- Una singola interfaccia può avere PIU' indirizzi IPv6 di qualsiasi tipo (unicast, anycast, multicast)
  - tutte le interfacce devono avere almeno un indirizzo di tipo "link-local unicast "

QUESTO CONCETTO E' **FONDAMENTALE** IN IPv6

Indirizzi IPv6

- L'uso di indirizzi "lunghi" e "multipli" per interfaccia permette di migliorare l'efficienza del routing
  - indirizzi più lunghi permettono l'aggregazione degli indirizzi per gerarchie e l'uso di tabelle di routing più piccole e più veloci da consultare
  - indirizzi multipli per interfaccia permettono ad un utente di usare diversi access provider attraverso la stessa interfaccia, e di avere diversi indirizzi aggregati per ogni provider

Sintassi degli indirizzi IPv6

- Per rappresentare formalmente gli indirizzi IPv6 si è scelto di suddividerli in 8 blocchi di 16 bit ciascuno
- I blocchi sono separati mediante il carattere ":" e vengono rappresentati in notazione esadecimale
- Un esempio di indirizzo IPv6 è:

  3FFE:1001:7654:3220:FEDC:BA98:789A:32AC
- Esistono delle semplificazioni:
  - si possono omettere gli zeri iniziali in ogni campo
  - si possono sostituire gruppi di zeri con "::"

Sintassi degli indirizzi IPv6

Esempio:

1080:0:0:0:8:800:200C:417A	unicast address
FF01:0:0:0:0:0:0:101	multicast address
0:0:0:0:0:0:0:1	loopback address
0:0:0:0:0:0:0:0	unspecified address

possono essere scritti come:

1080::8:800:200C:417A	unicast address
FF01::101	multicast address
::1	loopback address
::	unspecified address

Sintassi degli indirizzi IPv6

- Un modo alternativo di rappresentare indirizzi IPv6, specie in ambiente misti IPv4-IPv6 è:

  x:x:x:x:x:x:d.d.d.d

- x: valori esadecimali dei 6 blocchi da 16 bit più significativi
- d: valori decimali dei 4 blocchi da 8 bit meno significativi

Es. 0:0:0:0:0:0:13.1.68.3 IPv4-compatible IPv6 address

o in forma compressa:

::13.1.68.3

Prefissi IPv6

- IPv6 continua il modello IPv4 per cui ad un link può essere associato un subnet prefix. PIU' subnet prefix possono essere assegnati allo stesso link
- La rappresentazione del prefisso IPv6 è simile alla notazione CIDR dei prefissi IPv4:

  ipv6-address/prefix-length

  - ipv6-address è l'indirizzo IPv6 in una delle forme previste (anycast, multicast, unicast)
  - prefix-length è un valore decimale che specifica quanti dei bit contigui più significativi specificano il prefisso

Prefissi IPv6

Esempio:

il prefisso esadecimale di 60 bit 12AB00000000CD3 può essere rappresentato come:

12AB:0000:0000:CD30:0000:0000:0000:0000/60

12AB::CD30:0:0:0:0/60

12AB:0:0:CD30::/60

non sono legali le rappresentazioni seguenti:

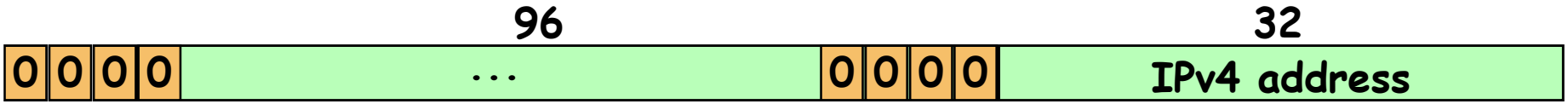
12AB:0:0:CD3/60 non si possono eliminare gli zeri in coda nei blocchi di 16 bit dell'indirizzo

12AB::CD30/60 l'indirizzo a sinistra di "/" si espanderebbe come:
12AB:0000:0000:0000:0000:000:0000:CD30

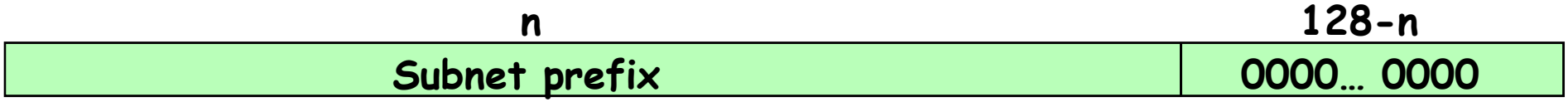
12AB::CD3/60 l'indirizzo a sinistra di "/" si espanderebbe come:
12AB:0000:0000:0000:0000:000:0000:0CD3

Formati di indirizzi IPv6

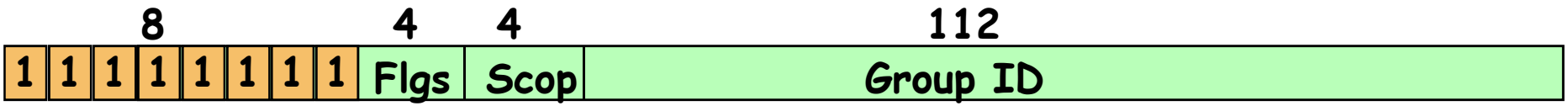
IPv4-compatible IPv6 address



Anycast address



Multicast address



Gerarchia di indirizzamento

- Gli indirizzi aggregabili sono organizzati in 3 livelli gerarchici:
  - Public Topology
  - Site Topology
  - Interface Identifier
- "Public topology" è l'insieme dei provider e delle centrali (exchange) che forniscono servizio di transito verso l'Internet pubblica
- "Site topology" è locale a un sito specifico o a un'organizzazione che non fornisce servizio di transito pubblico verso i nodi al di fuori del sito
- "Interface identifier" identifica le interfacce sui link

Extended Unique Identifier

OTTENUTO INT. ID A PARTIRE DALL'INDIRIZZO MAC:

EUI 48

MAC: 00:12:7F:EB:6A:31

- 00:12:7F → 24 Organizationally Unique Identifier
- EB:6A:31 → 24 Network Interface Card

1° STEP ⇒ 00:12:7F:FF:FE:EB:6A:3

si usa questa stringa fissa mi è ritorno l'utilizzo generalmente posto a 0 (come Global scope) lo pone a 1 per indicare un local scope

2° step: inversione del bit n.7 (universal/local flag)

00 ⇒ 02 ⇒ risultato finale:

02:12:7F:FF:FE:EB:6A:31

64 bit int. id