Security Topics

Arquitetura de Redes

Mestrado Integrado
Engenharia de Computadores e Telemática
DETI-UA

universidade de aveiro

deti.ua.pt

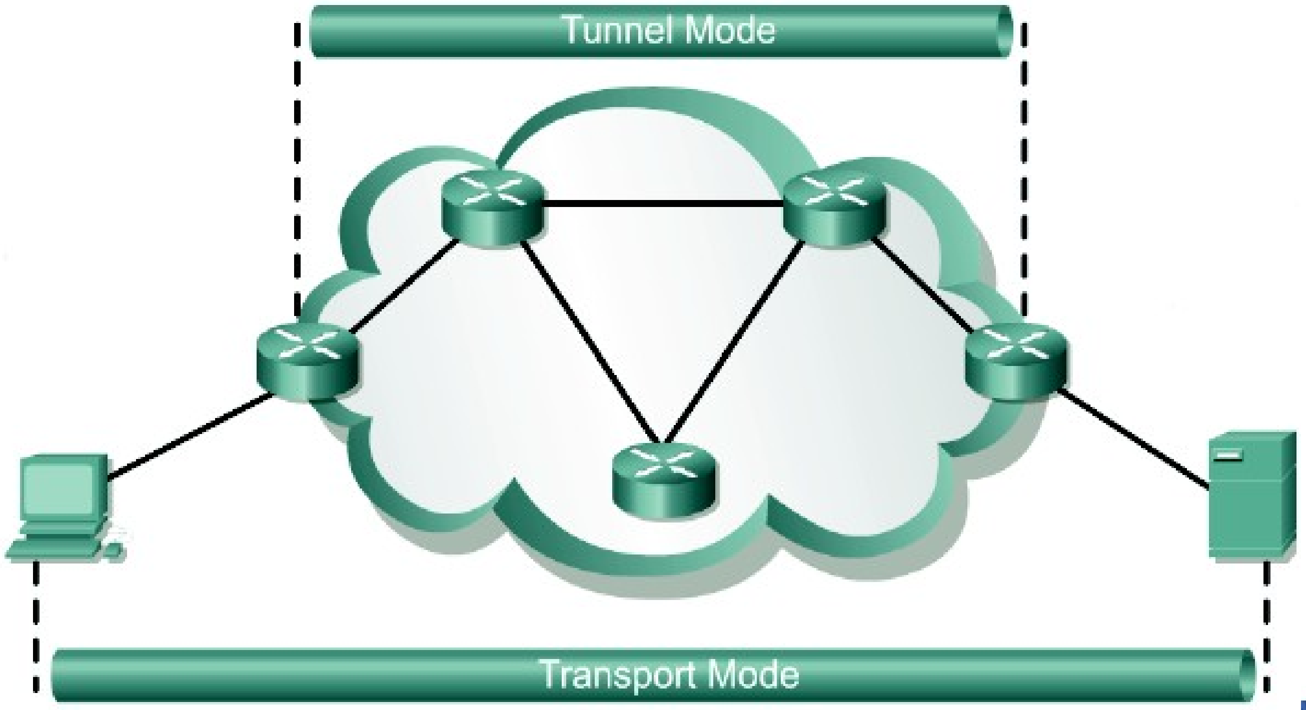
IP Secure Communications (IPsec Protocol)

IPSec

- Framework of security protocols and algorithms used to secure data at the network layer
- Authentication Header (AH)
  - Ensures data integrity
  - Does not provide confidentiality
  - Provides origin authentication
  - Uses Keyed-hash mechanisms
- Encapsulating Security Payload (ESP)
  - Provides data confidentiality (encryption)
  - Data Integrity
  - Does not protect IP header
- AH and ESP use symmetric secret key algorithms, although public key algorithms are feasible

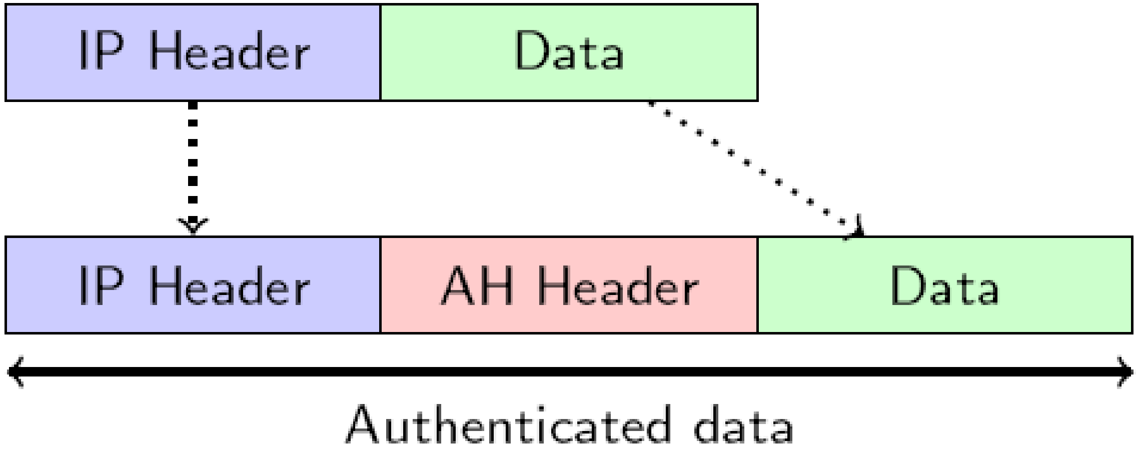
IPSec Modes

- Tunnel
  - IPSec gateways provide IPSec services to other hosts in peer-to-peer tunnels
  - End-hosts are not aware of IPSec being used to protect their traffic
  - IPSec gateways provide transparent protection over untrusted networks
- Transport
  - Each end host does IPSec encapsulation of its own data, host-to-host.
  - IPSec has to be implemented on end-hosts
  - The application endpoint must also be the IPSec endpoint

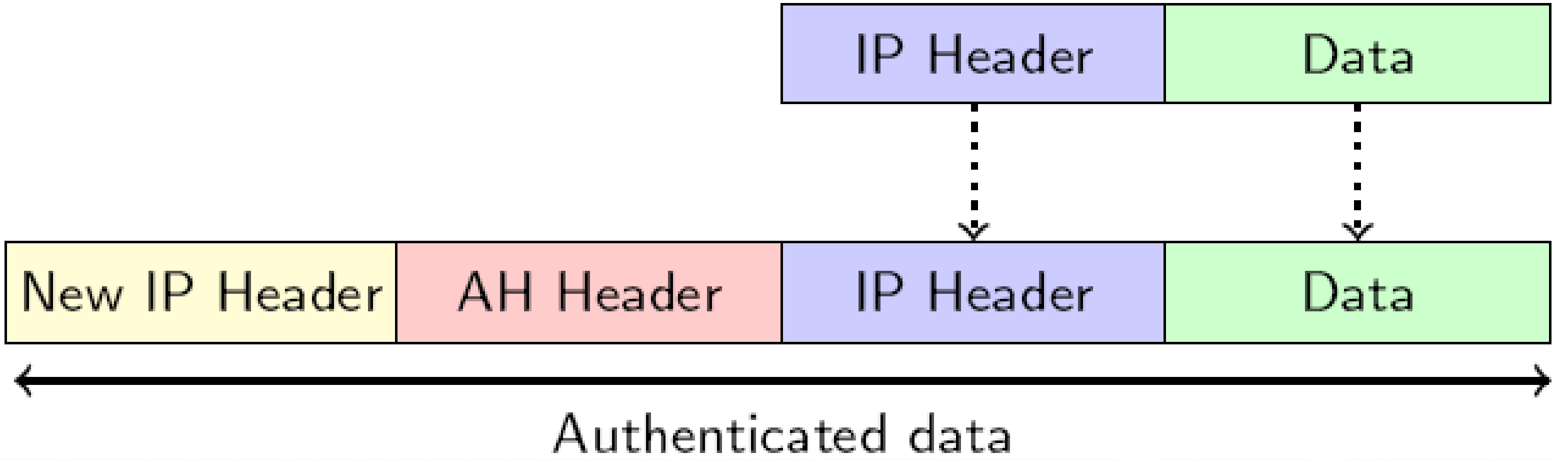


IPSec - AH header placement

- Transport mode

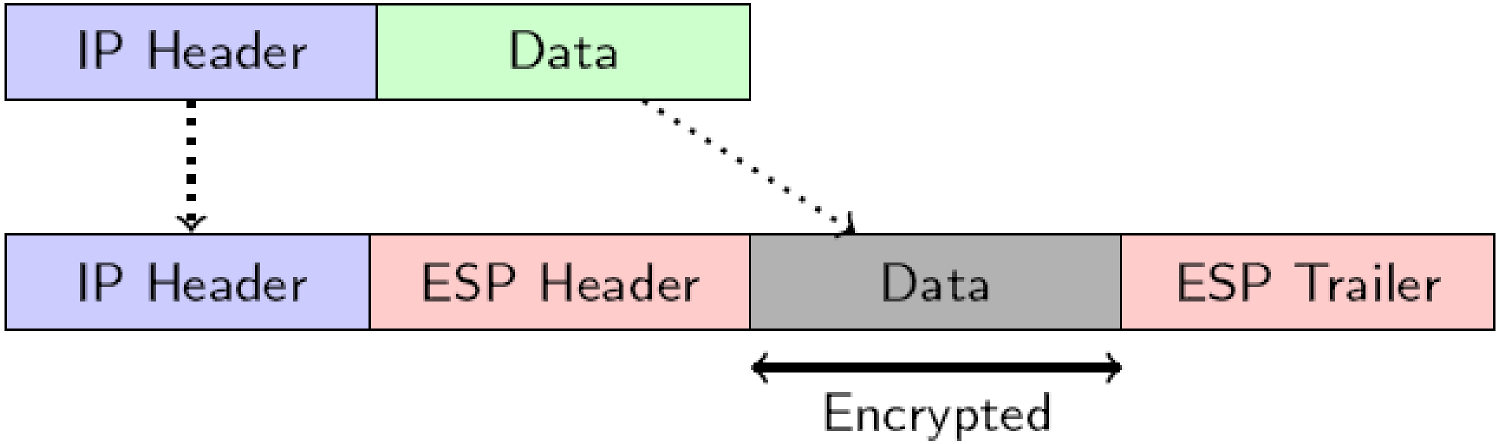


- Tunnel mode

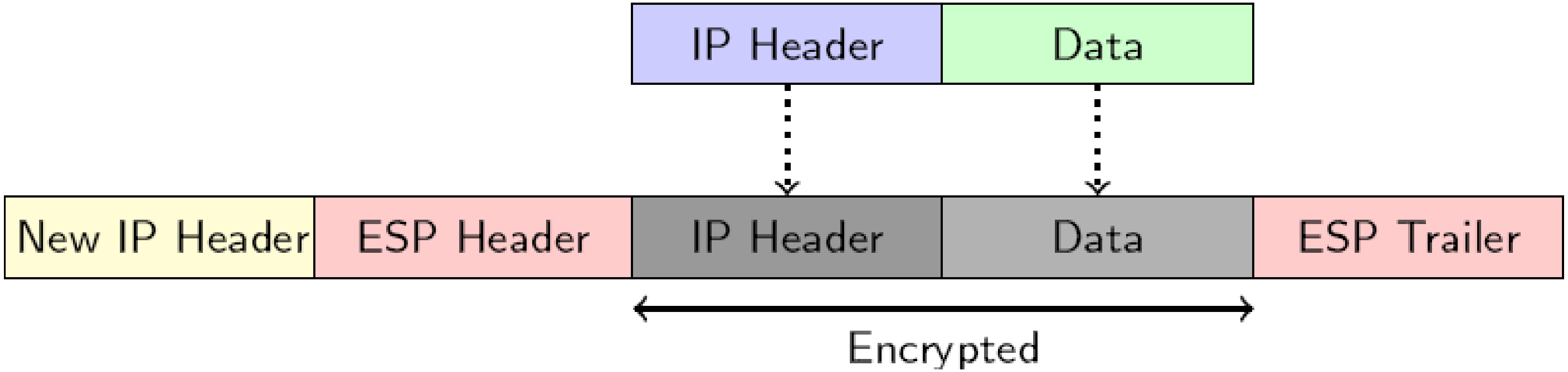


IPSec - ESP header placement

- Transport mode



- Tunnel mode



IPSec - Security Associations

- SAs represent a policy contract between two peers or hosts
- Describe how the peers will use IPSec security services to protect network traffic
- An SA contains the following security parameters:
  - Authentication/encryption algorithm, key length and other encryption parameters (e.g. key lifetime, ...)
  - Session keys for authentication, or HMACs, and encryption, which can be entered manually or negotiated automatically
  - A specification of network traffic to which the SA will be applied (e.g. IP traffic or only TELNET sessions)
  - IPSec AH or ESP encapsulation protocol and tunnel or transport mode

Establishing SA and Cryptographic Keys

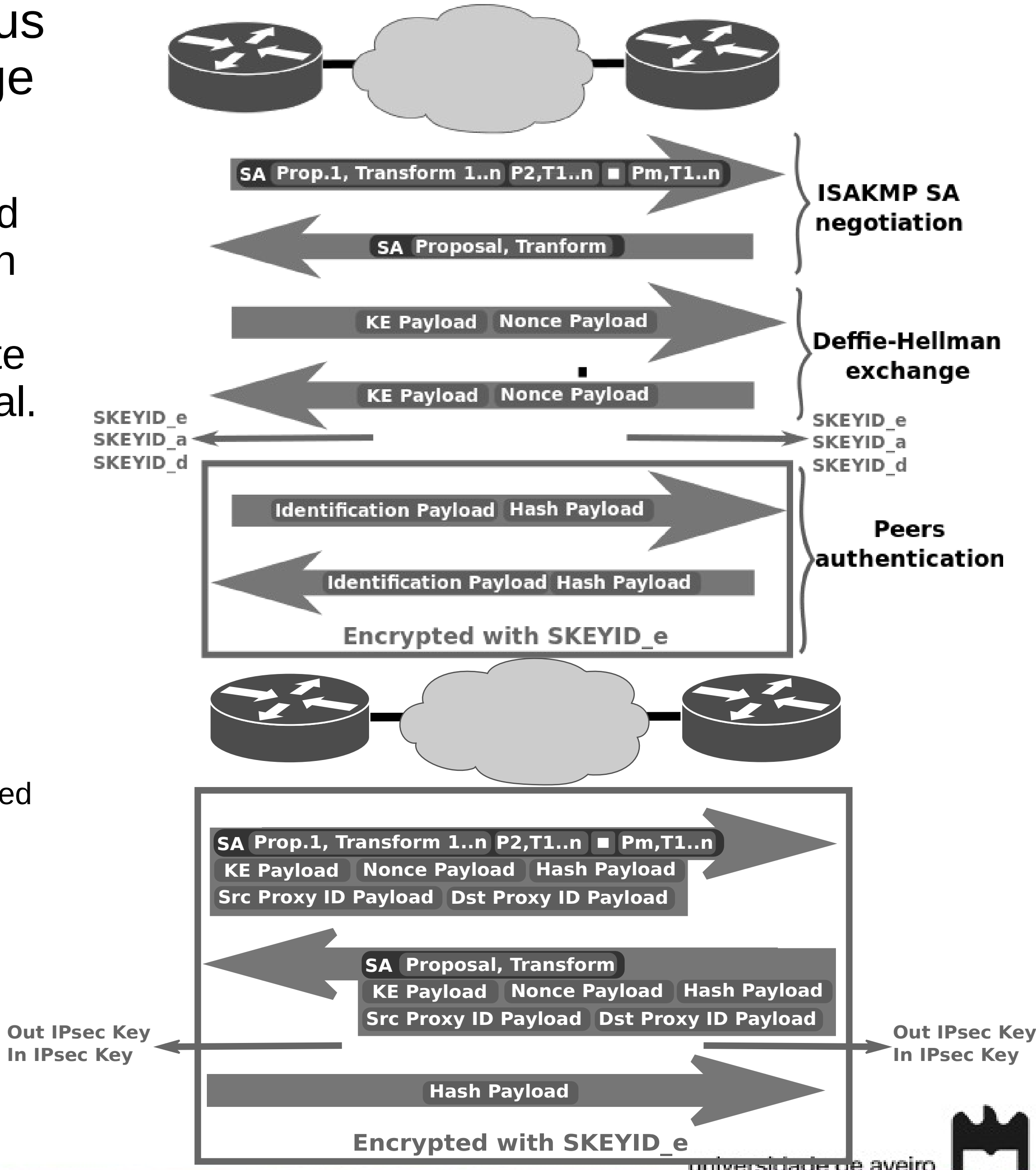
- ISAKMP - Internet Security Association and Key Management Protocol
  - Used to establishing Security Associations (SA) and cryptographic keys
  - Separate the details of security association management (and key management) from the details of key exchange
  - Provides a framework for authentication and key exchange but does not define them
- Oakley Key Determination Protocol
  - Key-agreement protocol
  - Allows authenticated peers to exchange keying material across an insecure connection
  - Uses Diffie-Hellman
- SKEME
  - Key exchange protocol
- IKE - Internet Key Exchange
  - Is a hybrid protocol
  - Uses part of Oakley and part of SKEME in conjunction with ISAKMP

IKE/ISAKMP and IPsec

- Enhances IPSec by providing additional features and flexibility
- Provides authentication of the IPSec peers, negotiates IPSec keys, and negotiates IPSec security associations
- The IKE tunnel protects the SA negotiations. After the SAs are in place, IPSec protects data transference
- Advantages
  - Eliminates the need to manually specify IPSec security parameters at both peers
  - Allows administrators to specify a lifetime for the IPSec security association
  - Allows encryption keys to change during IPSec sessions
  - Allows IPSec to provide anti-replay services
  - Permits certification authority (CA) support for a manageable, scalable IPSec implementation
  - Allows dynamic authentication of peers
- IKE/ISAKMP provides three methods for two-way authentication:
  - Pre-shared key (PSK),
  - Digital signatures (RSA-SIG),
  - Public key encryption (RSA-ENC).

ISAKMP and IPsec – Phases/Modes

- ISAKMP modes control an efficiency versus security tradeoff during initial key exchange
- Phase 1
  - Peer agree on a set of parameters to be used to authenticate peers and to encrypt a portion of the phase 1 exchanges and all of phase 2 exchanges, authenticate peers, and generate keys to be used as generating keying material.
  - Main mode
    - Requires six packets back and forth
    - Provides complete security during the establishment of an IPsec connection
    - Aggressive mode is an alternative to main mode
      - Uses half the exchanges, but provides less security because some information is transmitted in cleartext
- Phase 2 - Quick mode
  - Peers negotiate and agree on parameters required to establish a fully functional IPsec communication service.



SA Prop.1, Transform 1..n P2,T1..n ■ Pm,T1..n

SA Proposal, Tranform

ISAKMP SA negotiation

KE Payload Nonce Payload

KE Payload Nonce Payload

Deffie-Hellman exchange

SKEYID_e
SKEYID_a
SKEYID_d

SKEYID_e
SKEYID_a
SKEYID_d

Identification Payload Hash Payload

Identification Payload Hash Payload

Encrypted with SKEYID_e

Peers authentication

SA Prop.1, Transform 1..n P2,T1..n ■ Pm,T1..n
KE Payload Nonce Payload Hash Payload
Src Proxy ID Payload Dst Proxy ID Payload

SA Proposal, Transform
KE Payload Nonce Payload Hash Payload
Src Proxy ID Payload Dst Proxy ID Payload

Out IPsec Key
In IPsec Key

Out IPsec Key
In IPsec Key

Hash Payload

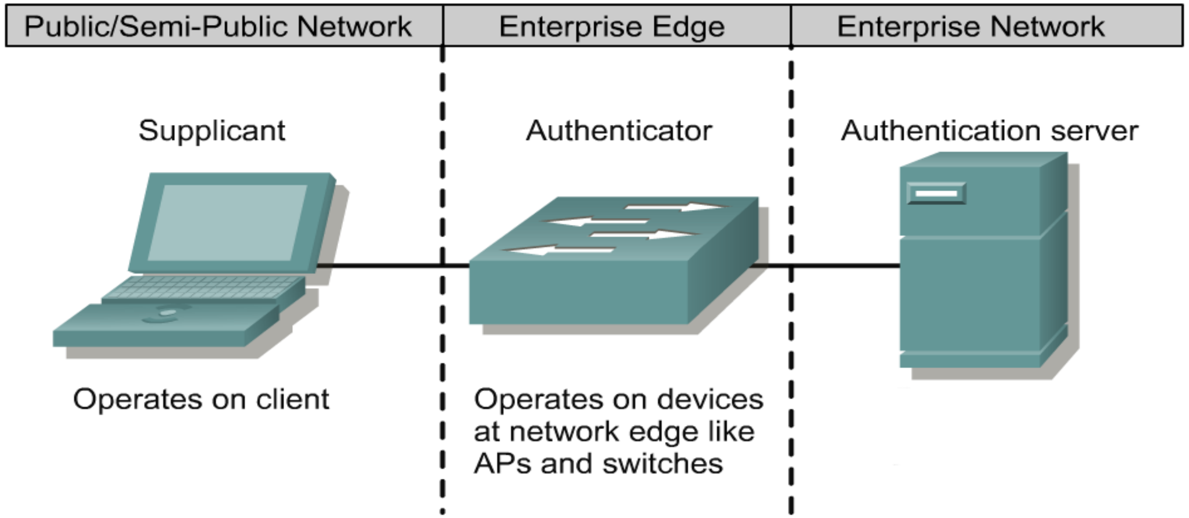
Encrypted with SKEYID_e

universidade de aveiro

Access Control

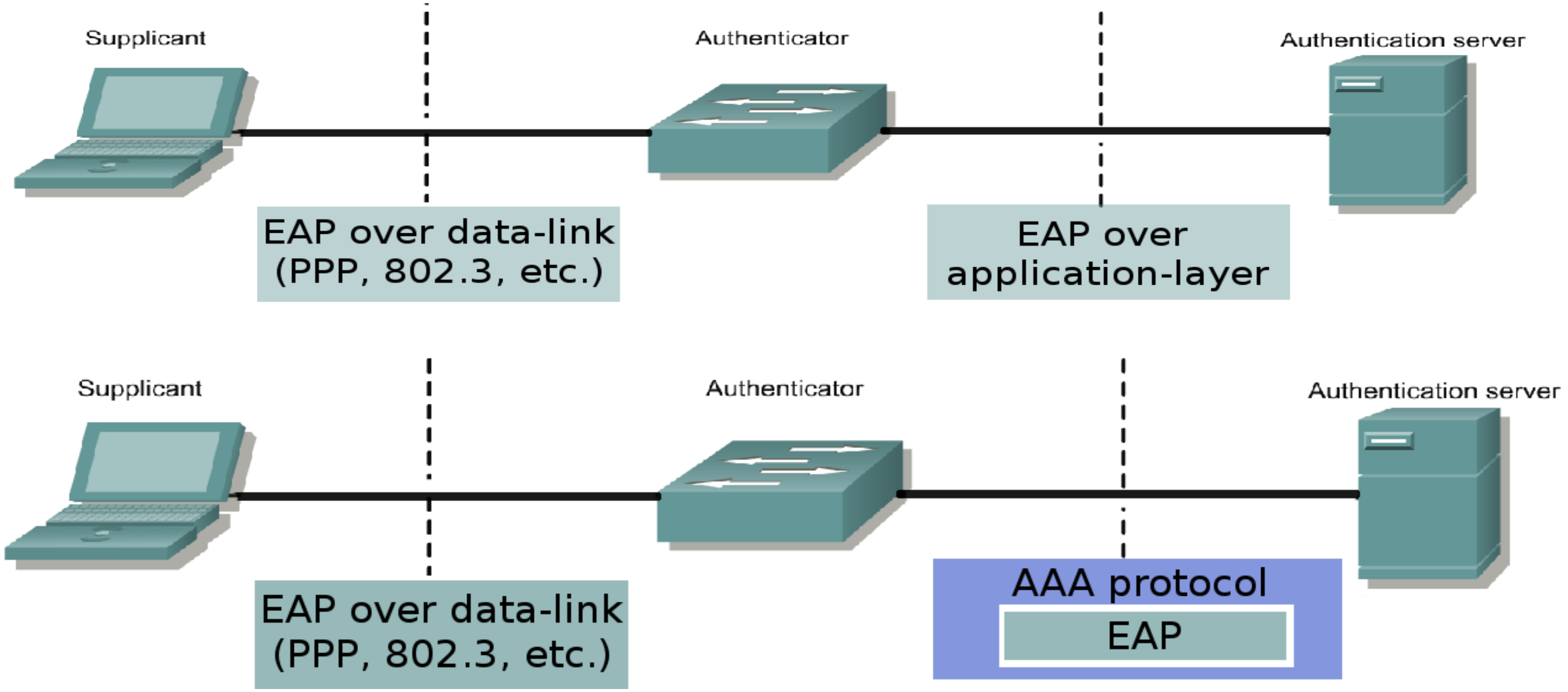
AAA Architecture

- Enables systematic access security
  - Authentication identifies an user
  - Authorization determines what that user can do
  - Accounting monitors the network usage time for billing purposes
- AAA information is typically stored in an external database or remote authentication server
- Traditional AAA Implementation



802.1X

- IEEE 802.1X is an IEEE Standard for Network Access Control (NAC)
  - 802.1X-2001 and 802.1X-2004 only provide authentication.
  - 802.1X-2010 adds optional encryption over the LAN segment.
- It provides an authentication mechanism to devices wishing to attach to a LAN.
- Based on the Extensible Authentication Protocol (EAP).
- AAA protocols/services: TACACS+, RADIUS and DIAMETER.



Extensible Authentication Protocol (EAP)

- EAP defined in [RFC3748] was designed to enable extensible authentication for network access in situations in which the Internet Protocol (IP) protocol is not available.
  - Originally developed for use with Point-to-Point Protocol (PPP) [RFC1661]
  - Subsequently also been applied to IEEE 802 wired networks [IEEE-802.1X], Internet Key Exchange Protocol version 2 (IKEv2)[RFC4306], and wireless networks such as [IEEE-802.11] and [IEEE-802.16e].
- EAP is a two-party protocol spoken between the EAP peer and server.
  - Keying material is generated by EAP authentication algorithms, known as "methods".
  - Part of this keying material can be used by EAP methods themselves, and part of this material can be exported.

EAP Overview (1)

- Where EAP key derivation is supported, the conversation typically takes place in three phases:
- Phase 0: Discovery
- Phase 1: Authentication
  - 1a: EAP authentication
  - 1b: AAA Key Transport (optional)
- Phase 2: Secure Association Protocol
  - 2a: Unicast Secure Association
  - 2b: Multicast Secure Association (optional)

EAP Overview (2)

- EAP lower layers implement phase 0, 2a, and 2b in different ways:
  - IEEE 802.1X
    - IEEE 802.1X-2004 does not support discovery (phase 0), nor does it provide for derivation of unicast or multicast secure associations (phase 2).
  - IEEE 802.11
    - Handles discovery via the Beacon and Probe Request/Response mechanisms.
    - Access Points (APs) periodically announce their Service Set Identifiers (SSIDs) as well as capabilities using Beacon frames.
    - Stations can query for APs by sending a Probe Request.
      - Neither Beacon nor Probe Request/Response frames are secured.
    - A 4-way handshake enables the derivation of unicast (phase 2a) and multicast/broadcast (phase 2b) secure associations.

EAP Overview (3)

- Common Methods
  - EAP-PSK - Mutual authentication and session key derivation using a Pre-Shared Key (PSK)
  - EAP-TLS - Uses PKI to secure communication to authentication server
  - PEAP - Protected EAP (PEAP) allows hybrid authentication. PEAP employs server-side PKI authentication. For client-side authentication, PEAP can use any other EAP authentication type.
  - EAP-TTLS -Client does not need be authenticated via a PKI certificate to the server, but only the server to the client
  - LEAP - Cisco’s proprietary EAP method. Uses a modified version of MS-CHAP
  - EAP over LAN (EAPoL) used in 802.1X.

TACACS+

- Terminal Access Controller Access Control System Plus
- Forwards username and password information to a centralized security server
- Centralized server can be either a TACACS database or a database like the UNIX password le with TACACS support
- Features
  - Separates all AAA functionalities
  - Uses TCP
  - Bidirectional authentication
  - All packet is encrypted
  - Limited accounting customization

RADIUS

- Remote Authentication Dial-In User Service
- The network access device operates as a client of RADIUS
- RADIUS servers are responsible for
  - Receiving user connection requests
  - Authenticating the user
  - Return all configuration information necessary for the client to deliver service to the user
- Transactions between the client and RADIUS server are authenticated using a shared secret
- Supports a variety of methods to authenticate a user
  - PAP, CHAP, or MS-CHAP, UNIX login, and other authentication mechanisms
- Combines Authentication and Authorization. Separates Accounting (less flexible than TACACS+)
- Uses UDP (less robust)
- Unidirectional authentication
- Only encrypts the password (less secure)
- RADIUS accounting can hold more information

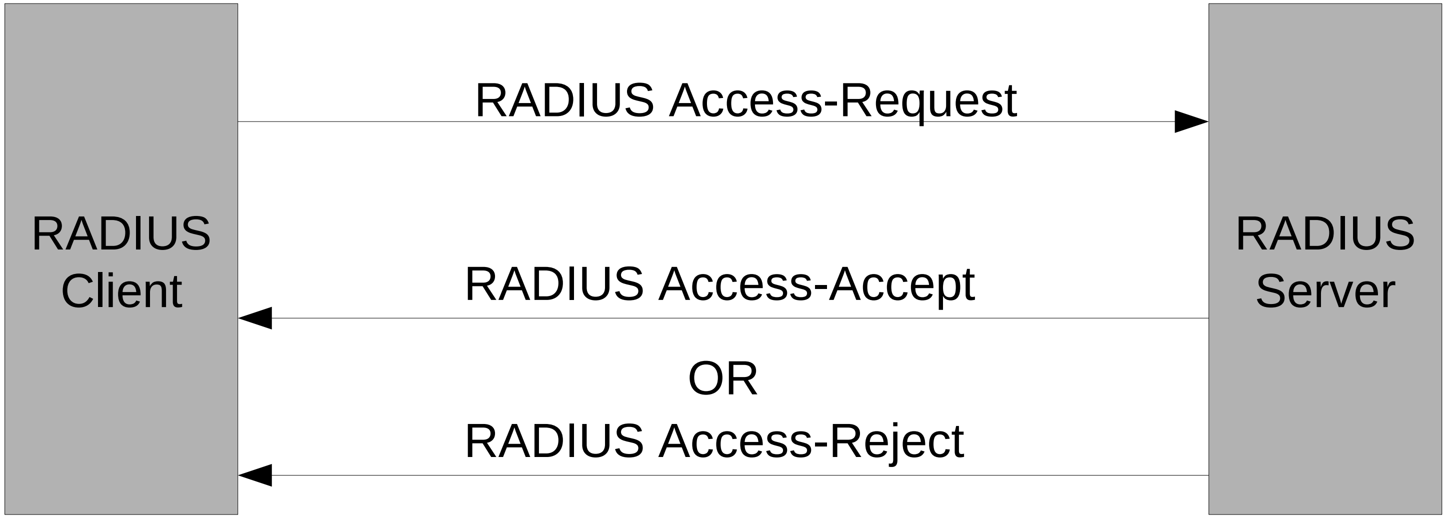
RADIUS Packet

<table>
<tr><td>Code (1 byte)</td><td>Identifier (1 byte)</td><td>Length (2 bytes)</td></tr>
<tr><td colspan="3">Authenticator (16 bytes)</td></tr>
<tr><td colspan="3">Attributes</td></tr>
</table>

- Code - Identifies the type of RADIUS packet
  - (1) Access-Request, (2) Access-Accept, (3) Access-Reject, (4) Accounting-Request, (5) Accounting-Response and (11) Access-Challenge
- Identifier - Allows the RADIUS client to match a RADIUS response with the correct pending request (usually is implemented as a counter)
- Authenticator
  - In client Requests – Random value
  - In server Responses - MD5 Hash function of (Code,ID,Length,Request Auth,Attributes,Shared Secret)
- Attributes - Section where an arbitrary number of attribute fields can be sent (e.g. User-Name and User-Password attributes)

RADIUS Protocol (1)

Example - RADIUS exchange involving just a username and user password:



- Only password is encrypted
  - The shared secret followed by the Request Authenticator is put through an MD5 hash to create a 16 octet value which is XORed with the password entered by the user
  - If the user password is greater than 16 octets, the password is broken into 16-octet blocks and additional MD5 calculations are performed

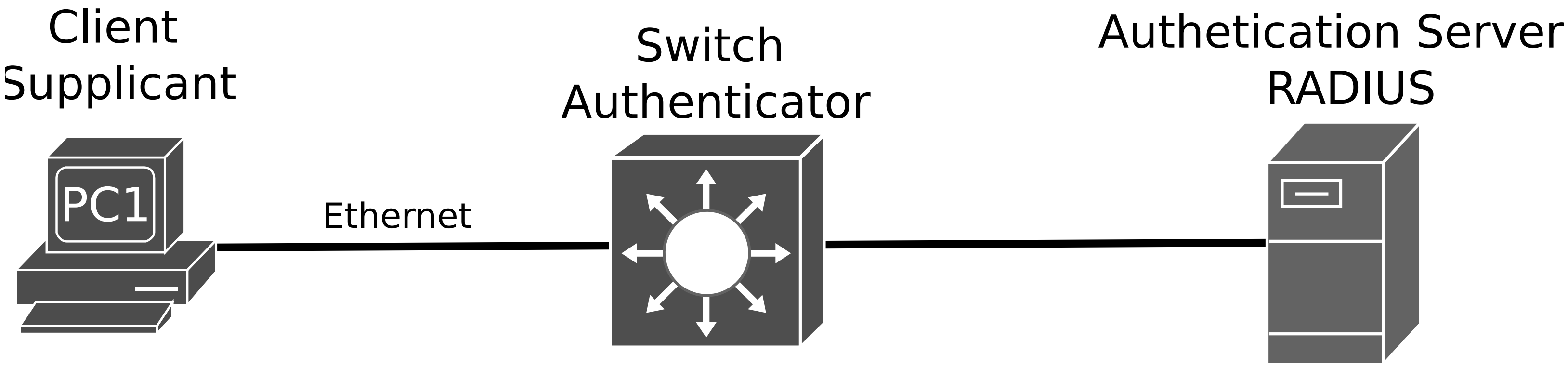
RADIUS Protocol (2)

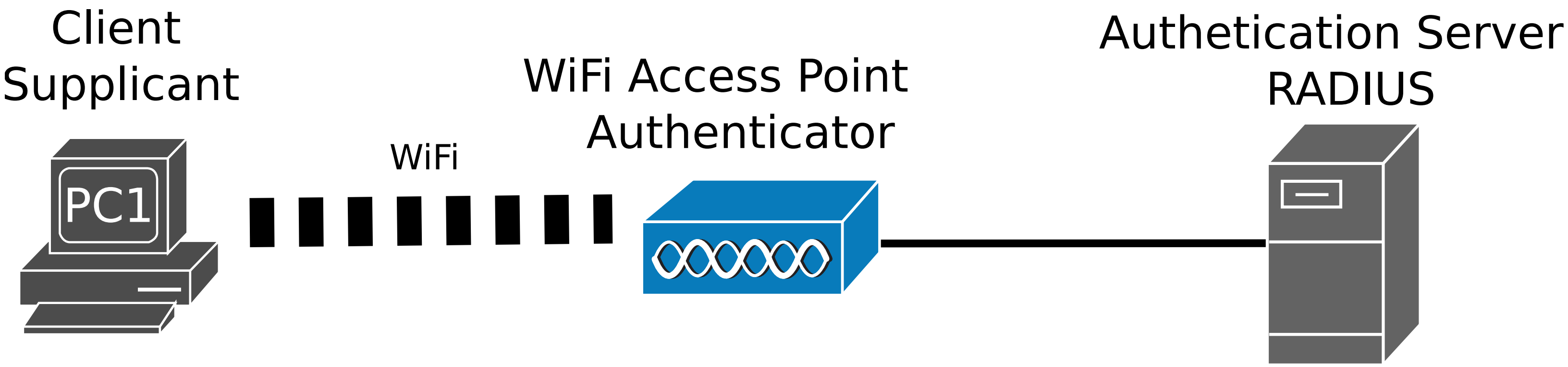
- The RADIUS protocol has a set of vulnerabilities
  - The Access-Request packet is not authenticated at all.
  - Many client implementations do not create Request Authenticators that are sufficiently random.
  - Many administrators choose RADIUS shared secrets with insufficient information entropy and many implementations limit the shared secret key space.

DIAMETER

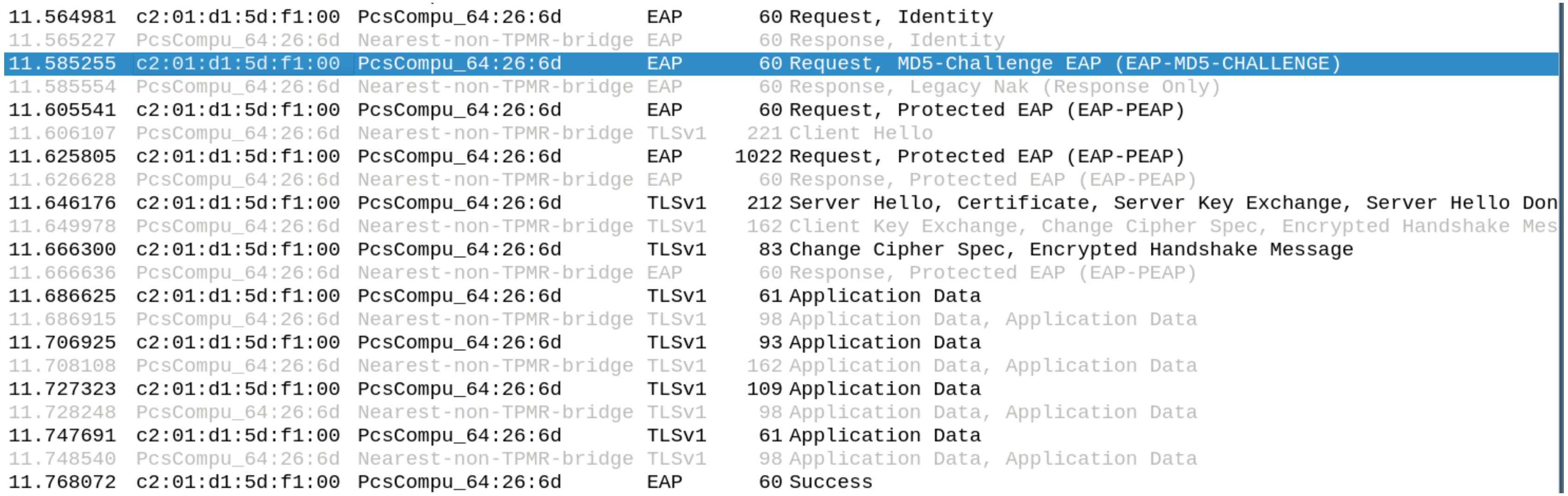
- DIAMETER is a newest framework in IETF for the next-generation AAA server
- Provides an AAA framework for Mobile-IP
- Does not use the same RADIUS protocol data unit, but is backward compatible with RADIUS to ease migration
- Bidirectional authentication
- It uses UDP but has a scheme that regulates the flow of packets
- Challenge/response attributes can be secured using end-to-end encryption and authentication
- Supports end-to-end security

802.1X - Ethernet vs. WiFi

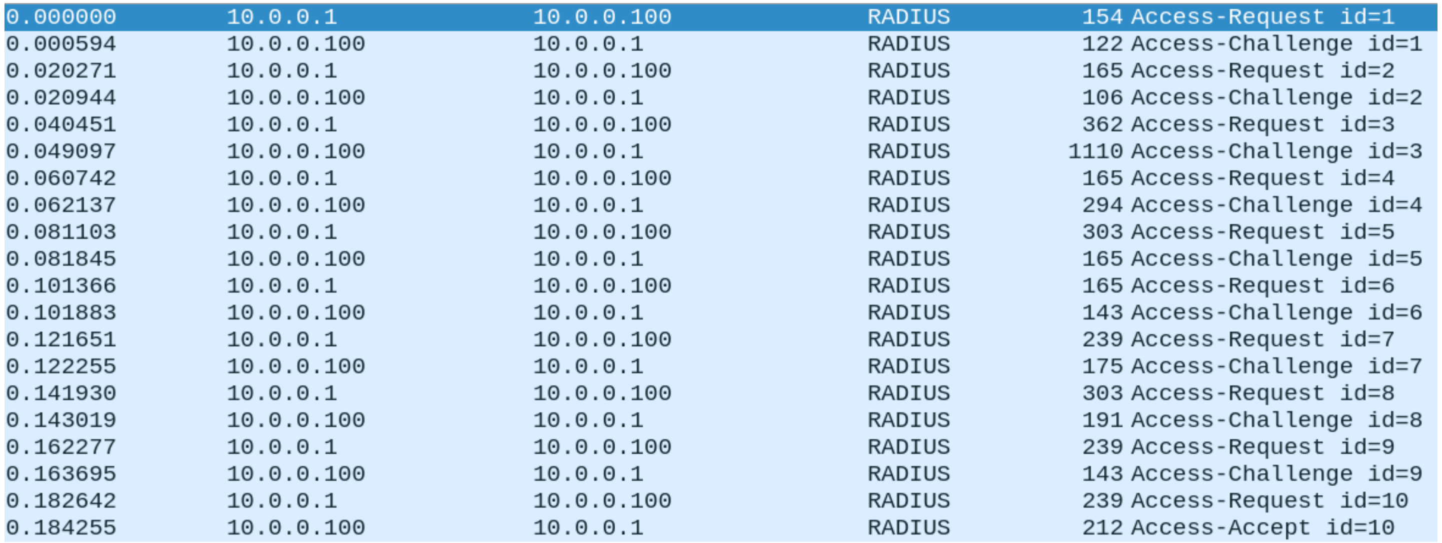




Ethernet - EAP and RADIUS



```
11.564981  c2:01:d1:5d:f1:00  PcsCompu_64:26:6d       EAP        60 Request, Identity
11.565227  PcsCompu_64:26:6d  Nearest-non-TPMR-bridge EAP        60 Response, Identity
11.585255  c2:01:d1:5d:f1:00  PcsCompu_64:26:6d       EAP        60 Request, MD5-Challenge EAP (EAP-MD5-CHALLENGE)
11.585554  PcsCompu_64:26:6d  Nearest-non-TPMR-bridge EAP        60 Response, Legacy Nak (Response Only)
11.605541  c2:01:d1:5d:f1:00  PcsCompu_64:26:6d       EAP        60 Request, Protected EAP (EAP-PEAP)
11.606107  PcsCompu_64:26:6d  Nearest-non-TPMR-bridge TLSv1     221 Client Hello
11.625805  c2:01:d1:5d:f1:00  PcsCompu_64:26:6d       EAP      1022 Request, Protected EAP (EAP-PEAP)
11.626628  PcsCompu_64:26:6d  Nearest-non-TPMR-bridge EAP        60 Response, Protected EAP (EAP-PEAP)
11.646176  c2:01:d1:5d:f1:00  PcsCompu_64:26:6d       TLSv1     212 Server Hello, Certificate, Server Key Exchange, Server Hello Don
11.649978  PcsCompu_64:26:6d  Nearest-non-TPMR-bridge TLSv1     162 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Mes
11.666300  c2:01:d1:5d:f1:00  PcsCompu_64:26:6d       TLSv1      83 Change Cipher Spec, Encrypted Handshake Message
11.666636  PcsCompu_64:26:6d  Nearest-non-TPMR-bridge EAP        60 Response, Protected EAP (EAP-PEAP)
11.686625  c2:01:d1:5d:f1:00  PcsCompu_64:26:6d       TLSv1      61 Application Data
11.686915  PcsCompu_64:26:6d  Nearest-non-TPMR-bridge TLSv1      98 Application Data, Application Data
11.706925  c2:01:d1:5d:f1:00  PcsCompu_64:26:6d       TLSv1      93 Application Data
11.708108  PcsCompu_64:26:6d  Nearest-non-TPMR-bridge TLSv1     162 Application Data, Application Data
11.727323  c2:01:d1:5d:f1:00  PcsCompu_64:26:6d       TLSv1     109 Application Data
11.728248  PcsCompu_64:26:6d  Nearest-non-TPMR-bridge TLSv1      98 Application Data, Application Data
11.747691  c2:01:d1:5d:f1:00  PcsCompu_64:26:6d       TLSv1      61 Application Data
11.748540  PcsCompu_64:26:6d  Nearest-non-TPMR-bridge TLSv1      98 Application Data, Application Data
11.768072  c2:01:d1:5d:f1:00  PcsCompu_64:26:6d       EAP        60 Success
```



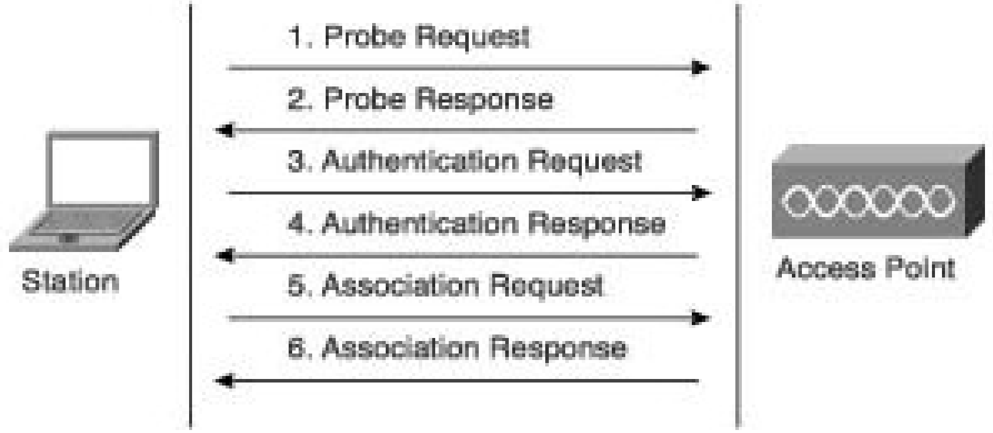
```
0.000000    10.0.0.1      10.0.0.100    RADIUS     154 Access-Request id=1
0.000594    10.0.0.100    10.0.0.1      RADIUS     122 Access-Challenge id=1
0.020271    10.0.0.1      10.0.0.100    RADIUS     165 Access-Request id=2
0.020944    10.0.0.100    10.0.0.1      RADIUS     106 Access-Challenge id=2
0.040451    10.0.0.1      10.0.0.100    RADIUS     362 Access-Request id=3
0.049097    10.0.0.100    10.0.0.1      RADIUS    1110 Access-Challenge id=3
0.060742    10.0.0.1      10.0.0.100    RADIUS     165 Access-Request id=4
0.062137    10.0.0.100    10.0.0.1      RADIUS     294 Access-Challenge id=4
0.081103    10.0.0.1      10.0.0.100    RADIUS     303 Access-Request id=5
0.081845    10.0.0.100    10.0.0.1      RADIUS     165 Access-Challenge id=5
0.101366    10.0.0.1      10.0.0.100    RADIUS     165 Access-Request id=6
0.101883    10.0.0.100    10.0.0.1      RADIUS     143 Access-Challenge id=6
0.121651    10.0.0.1      10.0.0.100    RADIUS     239 Access-Request id=7
0.122255    10.0.0.100    10.0.0.1      RADIUS     175 Access-Challenge id=7
0.141930    10.0.0.1      10.0.0.100    RADIUS     303 Access-Request id=8
0.143019    10.0.0.100    10.0.0.1      RADIUS     191 Access-Challenge id=8
0.162277    10.0.0.1      10.0.0.100    RADIUS     239 Access-Request id=9
0.163695    10.0.0.100    10.0.0.1      RADIUS     143 Access-Challenge id=9
0.182642    10.0.0.1      10.0.0.100    RADIUS     239 Access-Request id=10
0.184255    10.0.0.100    10.0.0.1      RADIUS     212 Access-Accept id=10
```

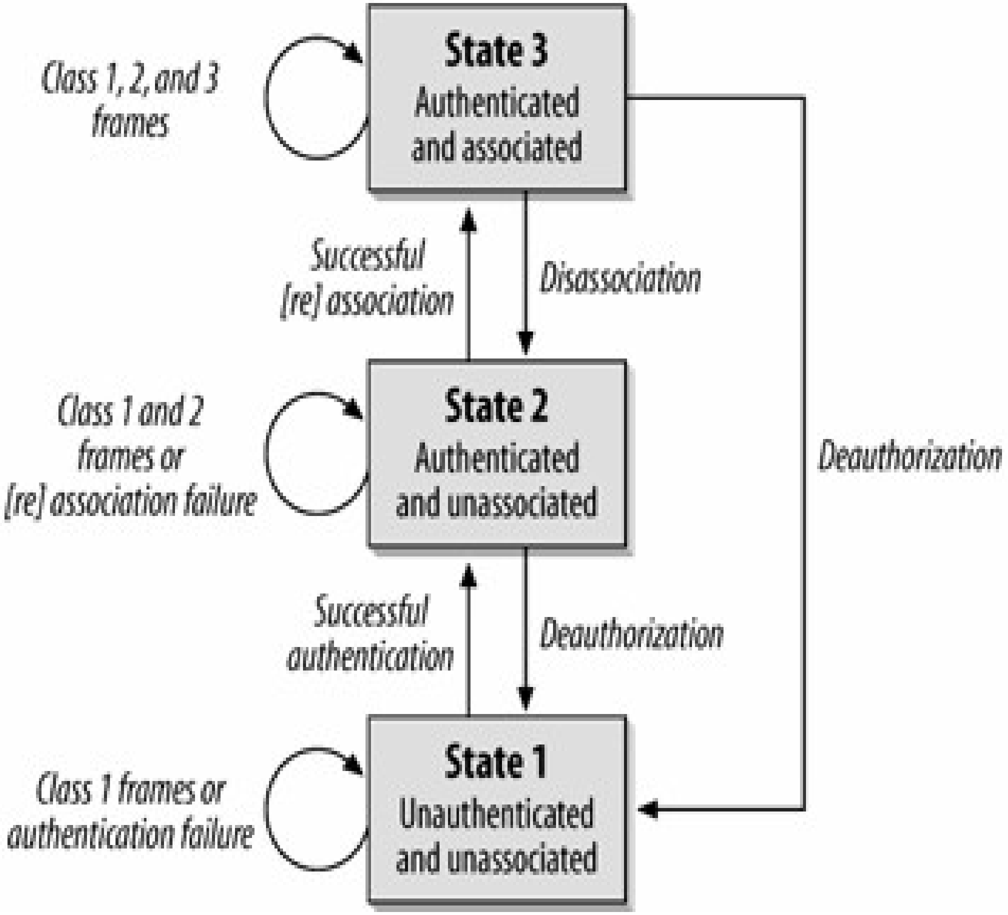
IEEE 802.11 services

- Station services (similar to wired network)
  - Authentication (login)
  - De-authentication (logout)
  - Privacy
  - Data delivery
- Distribution services
  - Association
    - Make logical connection between the AP and the station – the AP will not receive any data from a station before association
  - Re-association (similar to association)
    - Send repeatedly to the AP.
    - Help the AP to know if the station has moved from/to another BSS.
    - After Power Save
  - Disassociation
    - Manually disconnect (PC is shutdown or adapter is ejected)

Joining a BSS

- Station finds BSS/AP by **Scanning/Probing**.
- BSS with AP: both **Authentication** and **Association** are necessary for joining a BSS.

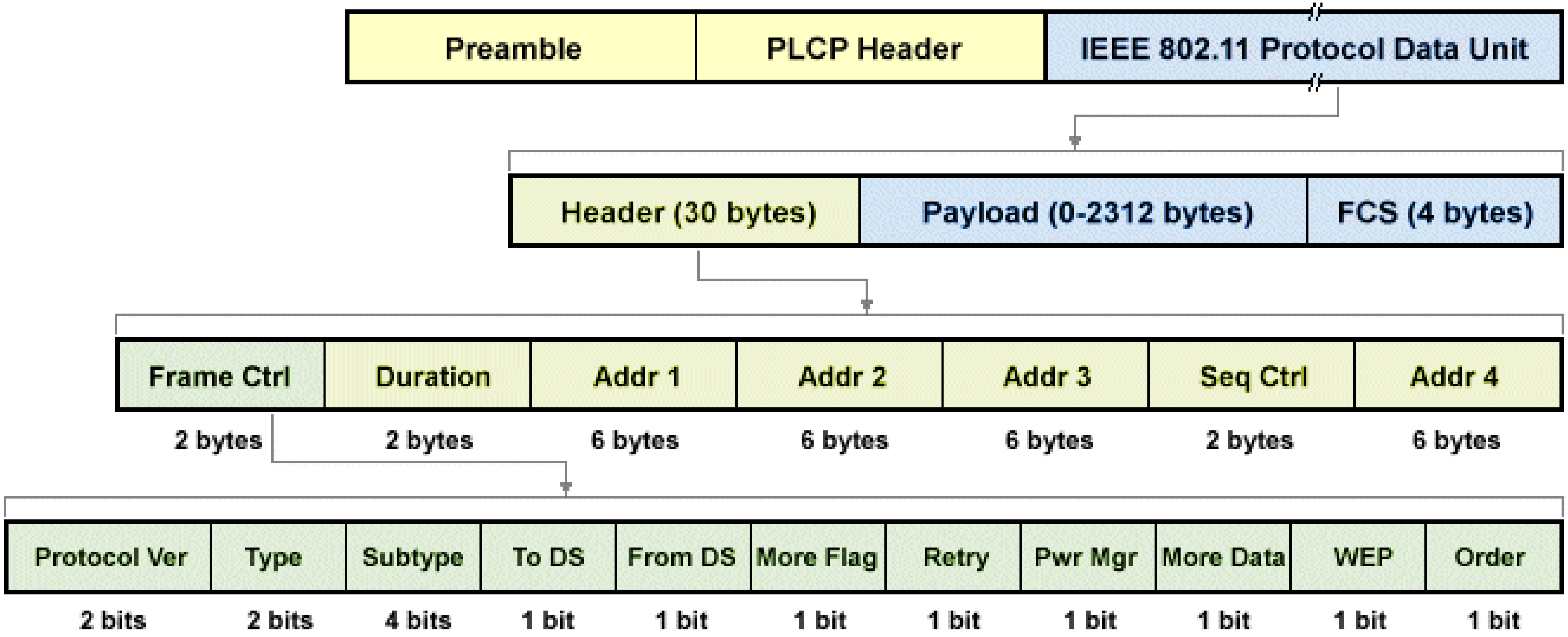




State 3
Authenticated and associated
Class 1, 2, and 3 frames
Successful [re] association
Disassociation
State 2
Authenticated and unassociated
Class 1 and 2 frames or [re] association failure
Deauthorization
Successful authentication
Deauthorization
State 1
Unauthenticated and unassociated
Class 1 frames or authentication failure

WLAN Frames

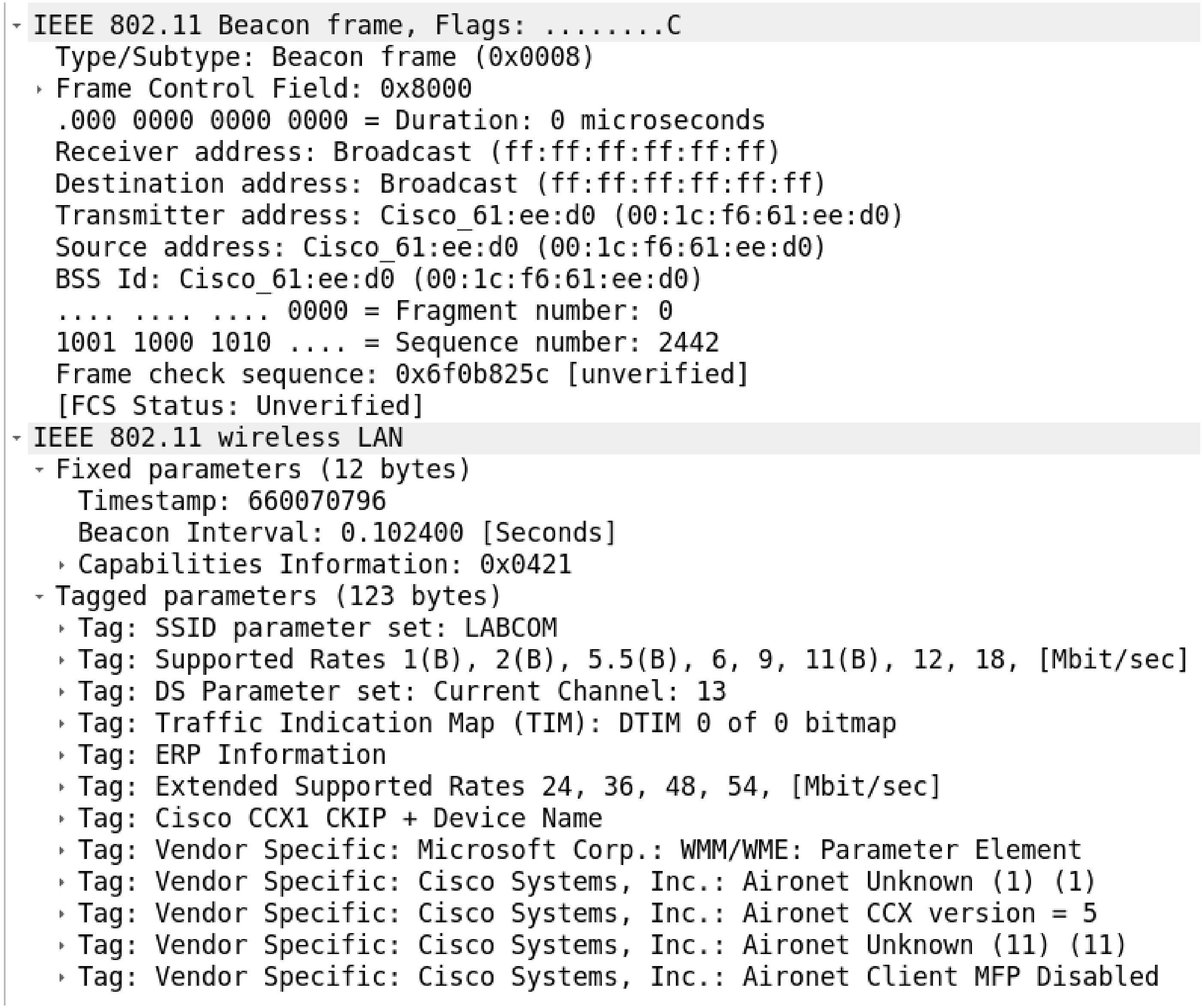
- Three types of frames
  - Control: RTS, CTS, ACK
  - Management
  - Data
- Header is different for the different types of frames.



Joining BSS with AP: Scanning

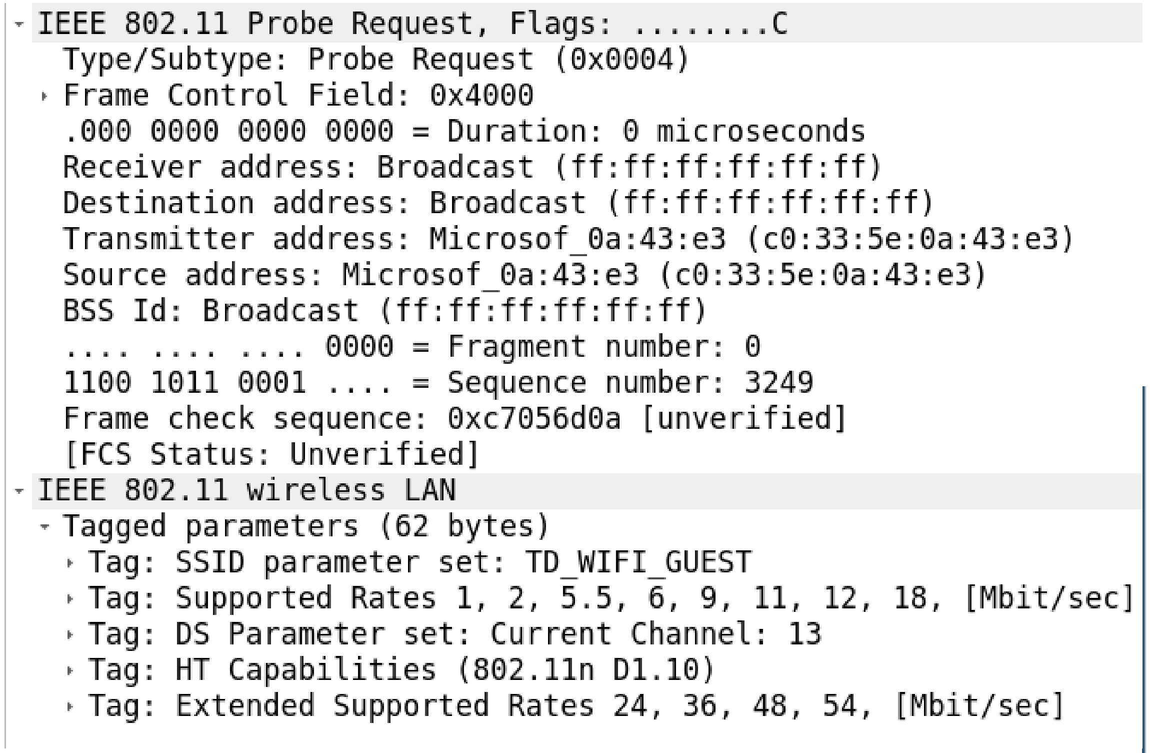
- A station willing to join a BSS must get in contact with the AP. This can happen through:
- 1. Passive scanning
  - The station scans the channels for a Beacon frame that is sent periodically from an AP to announce its presence and provide the SSID, and other parameters for WNICs within range
- 2. Active scanning (the station tries to find an AP)
  - The station sends a Probe Request frame - Sent from a station when it requires information from another station
  - All AP’s within reach reply with a Probe Response frame - Sent from an AP containing capability information, supported data rates, etc., after receiving a probe request frame

Beacon Frame

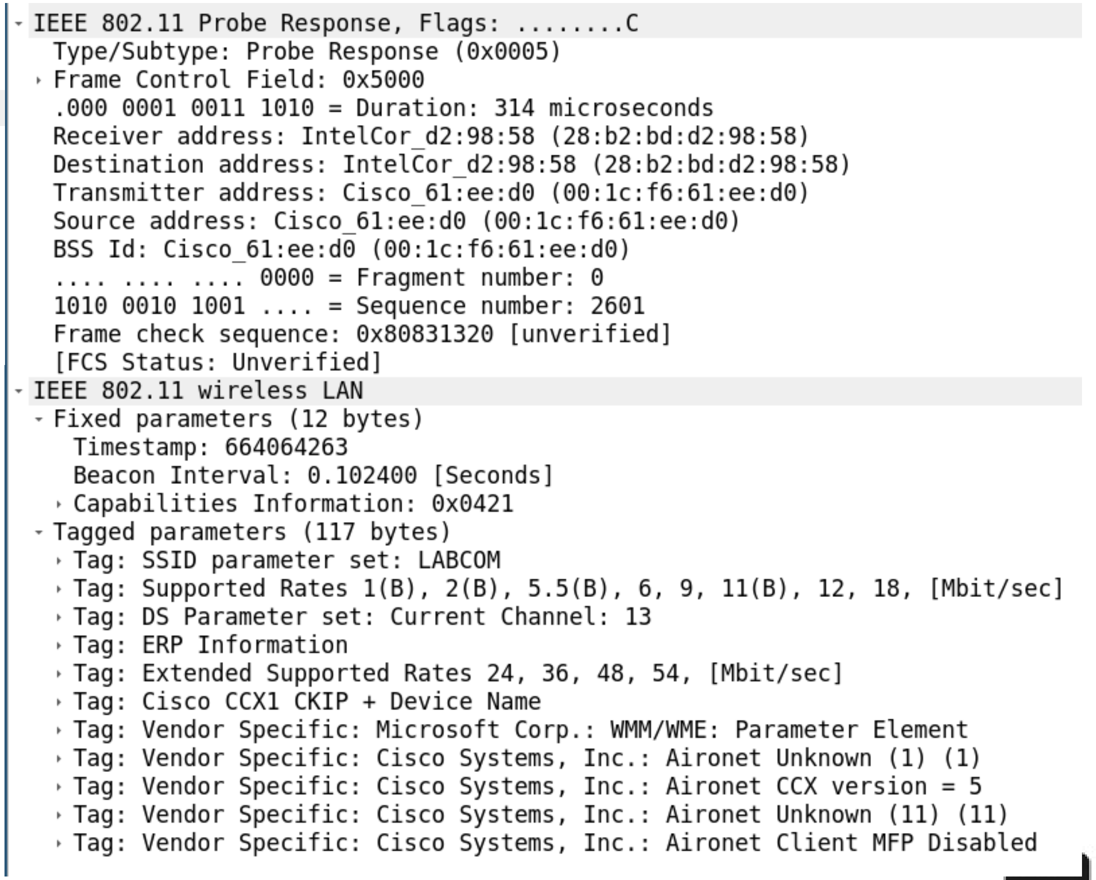


```
▾ IEEE 802.11 Beacon frame, Flags: ........C
    Type/Subtype: Beacon frame (0x0008)
  ▸ Frame Control Field: 0x8000
    .000 0000 0000 0000 = Duration: 0 microseconds
    Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
    Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
    Transmitter address: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
    Source address: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
    BSS Id: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
    .... .... .... 0000 = Fragment number: 0
    1001 1000 1010 .... = Sequence number: 2442
    Frame check sequence: 0x6f0b825c [unverified]
    [FCS Status: Unverified]
▾ IEEE 802.11 wireless LAN
  ▾ Fixed parameters (12 bytes)
      Timestamp: 660070796
      Beacon Interval: 0.102400 [Seconds]
    ▸ Capabilities Information: 0x0421
  ▾ Tagged parameters (123 bytes)
    ▸ Tag: SSID parameter set: LABCOM
    ▸ Tag: Supported Rates 1(B), 2(B), 5.5(B), 6, 9, 11(B), 12, 18, [Mbit/sec]
    ▸ Tag: DS Parameter set: Current Channel: 13
    ▸ Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
    ▸ Tag: ERP Information
    ▸ Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]
    ▸ Tag: Cisco CCX1 CKIP + Device Name
    ▸ Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
    ▸ Tag: Vendor Specific: Cisco Systems, Inc.: Aironet Unknown (1) (1)
    ▸ Tag: Vendor Specific: Cisco Systems, Inc.: Aironet CCX version = 5
    ▸ Tag: Vendor Specific: Cisco Systems, Inc.: Aironet Unknown (11) (11)
    ▸ Tag: Vendor Specific: Cisco Systems, Inc.: Aironet Client MFP Disabled
```

Probe Request/Response Frames



```
▾ IEEE 802.11 Probe Request, Flags: ........C
    Type/Subtype: Probe Request (0x0004)
  ▸ Frame Control Field: 0x4000
    .000 0000 0000 0000 = Duration: 0 microseconds
    Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
    Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
    Transmitter address: Microsof_0a:43:e3 (c0:33:5e:0a:43:e3)
    Source address: Microsof_0a:43:e3 (c0:33:5e:0a:43:e3)
    BSS Id: Broadcast (ff:ff:ff:ff:ff:ff)
    .... .... .... 0000 = Fragment number: 0
    1100 1011 0001 .... = Sequence number: 3249
    Frame check sequence: 0xc7056d0a [unverified]
    [FCS Status: Unverified]
▾ IEEE 802.11 wireless LAN
  ▾ Tagged parameters (62 bytes)
    ▸ Tag: SSID parameter set: TD_WIFI_GUEST
    ▸ Tag: Supported Rates 1, 2, 5.5, 6, 9, 11, 12, 18, [Mbit/sec]
    ▸ Tag: DS Parameter set: Current Channel: 13
    ▸ Tag: HT Capabilities (802.11n D1.10)
    ▸ Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]
```



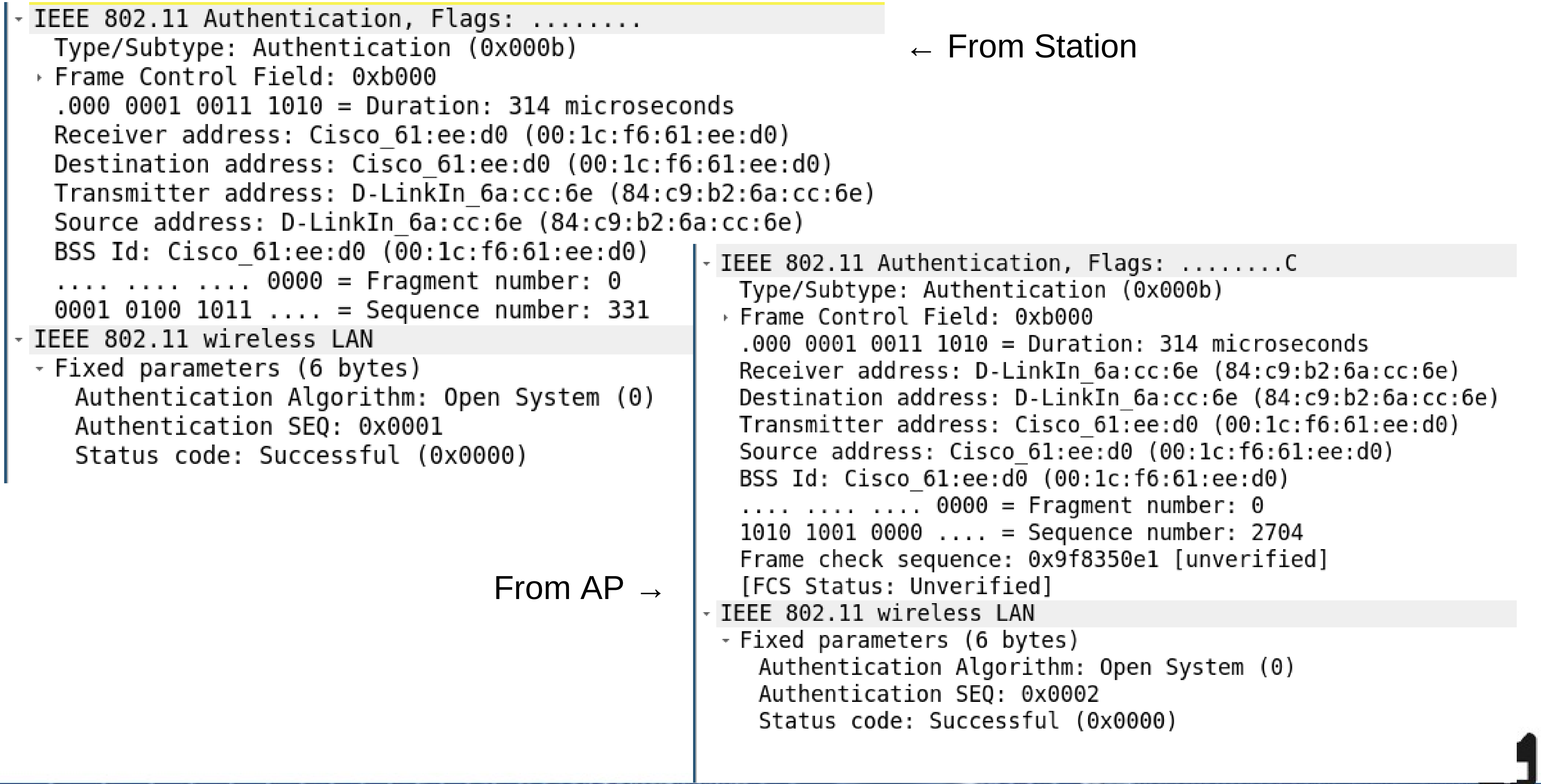
```
▾ IEEE 802.11 Probe Response, Flags: ........C
    Type/Subtype: Probe Response (0x0005)
  ▸ Frame Control Field: 0x5000
    .000 0001 0011 1010 = Duration: 314 microseconds
    Receiver address: IntelCor_d2:98:58 (28:b2:bd:d2:98:58)
    Destination address: IntelCor_d2:98:58 (28:b2:bd:d2:98:58)
    Transmitter address: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
    Source address: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
    BSS Id: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
    .... .... .... 0000 = Fragment number: 0
    1010 0010 1001 .... = Sequence number: 2601
    Frame check sequence: 0x80831320 [unverified]
    [FCS Status: Unverified]
▾ IEEE 802.11 wireless LAN
  ▾ Fixed parameters (12 bytes)
      Timestamp: 664064263
      Beacon Interval: 0.102400 [Seconds]
    ▸ Capabilities Information: 0x0421
  ▾ Tagged parameters (117 bytes)
    ▸ Tag: SSID parameter set: LABCOM
    ▸ Tag: Supported Rates 1(B), 2(B), 5.5(B), 6, 9, 11(B), 12, 18, [Mbit/sec]
    ▸ Tag: DS Parameter set: Current Channel: 13
    ▸ Tag: ERP Information
    ▸ Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]
    ▸ Tag: Cisco CCX1 CKIP + Device Name
    ▸ Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
    ▸ Tag: Vendor Specific: Cisco Systems, Inc.: Aironet Unknown (1) (1)
    ▸ Tag: Vendor Specific: Cisco Systems, Inc.: Aironet CCX version = 5
    ▸ Tag: Vendor Specific: Cisco Systems, Inc.: Aironet Unknown (11) (11)
    ▸ Tag: Vendor Specific: Cisco Systems, Inc.: Aironet Client MFP Disabled
```

Joining BSS with AP: Authentication

- Once an AP is found/selected, a station goes through authentication
- Open system authentication (default, 2-step process)
  - Station sends authentication frame with its identity
  - AP sends frame as an Ack / NAck
- Shared key authentication
  - Stations receive shared secret key through secure channel independent of 802.11
  - After the WNIC sends its initial authentication request, it will receive an authentication frame from the AP containing a challenge text
  - The WNIC sends an authentication frame containing the encrypted version of the challenge text to the AP.
  - The AP ensures the text was encrypted with the correct key by decrypting it with its own key.
  - The result of this process determines the WNIC's authentication status.

Authentication Frames

- Nowadays, WPA* sedcure networks use “Open System”.
- Non-”Open System” authentication was used for WEP protected networks (unsecured and functionally deprecated).



```
▾ IEEE 802.11 Authentication, Flags: ........
    Type/Subtype: Authentication (0x000b)
  ▸ Frame Control Field: 0xb000
    .000 0001 0011 1010 = Duration: 314 microseconds
    Receiver address: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
    Destination address: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
    Transmitter address: D-LinkIn_6a:cc:6e (84:c9:b2:6a:cc:6e)
    Source address: D-LinkIn_6a:cc:6e (84:c9:b2:6a:cc:6e)
    BSS Id: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
    .... .... .... 0000 = Fragment number: 0
    0001 0100 1011 .... = Sequence number: 331
▾ IEEE 802.11 wireless LAN
  ▾ Fixed parameters (6 bytes)
      Authentication Algorithm: Open System (0)
      Authentication SEQ: 0x0001
      Status code: Successful (0x0000)
```

← From Station

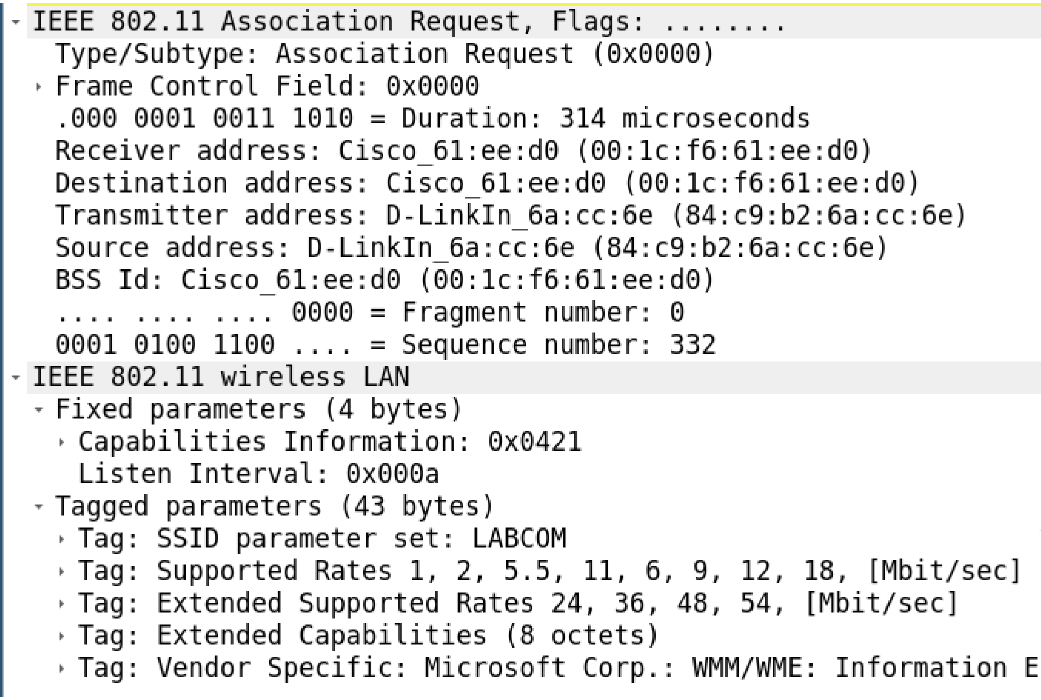
From AP →

```
▾ IEEE 802.11 Authentication, Flags: ........C
    Type/Subtype: Authentication (0x000b)
  ▸ Frame Control Field: 0xb000
    .000 0001 0011 1010 = Duration: 314 microseconds
    Receiver address: D-LinkIn_6a:cc:6e (84:c9:b2:6a:cc:6e)
    Destination address: D-LinkIn_6a:cc:6e (84:c9:b2:6a:cc:6e)
    Transmitter address: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
    Source address: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
    BSS Id: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
    .... .... .... 0000 = Fragment number: 0
    1010 1001 0000 .... = Sequence number: 2704
    Frame check sequence: 0x9f8350e1 [unverified]
    [FCS Status: Unverified]
▾ IEEE 802.11 wireless LAN
  ▾ Fixed parameters (6 bytes)
      Authentication Algorithm: Open System (0)
      Authentication SEQ: 0x0002
      Status code: Successful (0x0000)
```

Joining BSS with AP: Association

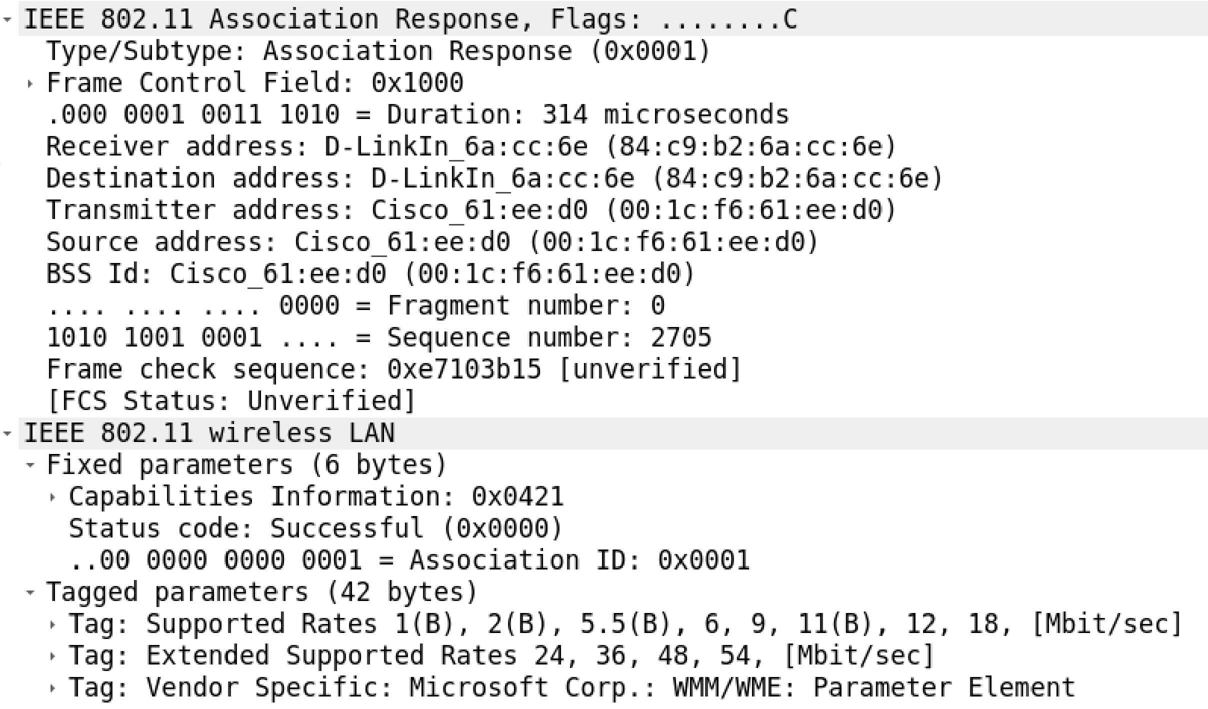
- Once a station is authenticated, it starts the association process, i.e., information exchange about the AP/station capabilities and roaming
  - STA → AP: Associate Request frame
    - Enables the AP to allocate resources and synchronize. The frame carries information about the WNIC, including supported data rates and the SSID of the network the station wishes to associate with.
  - AP → STA: Association Response frame
    - Acceptance or rejection to an association request. If it is an acceptance, the frame will contain information such as association ID and supported data rates.
  - New AP informs old AP (if it is a handover).
- Only after association is completed, a station can transmit and receive data frames.

Association Request/Response Frames



← From Station

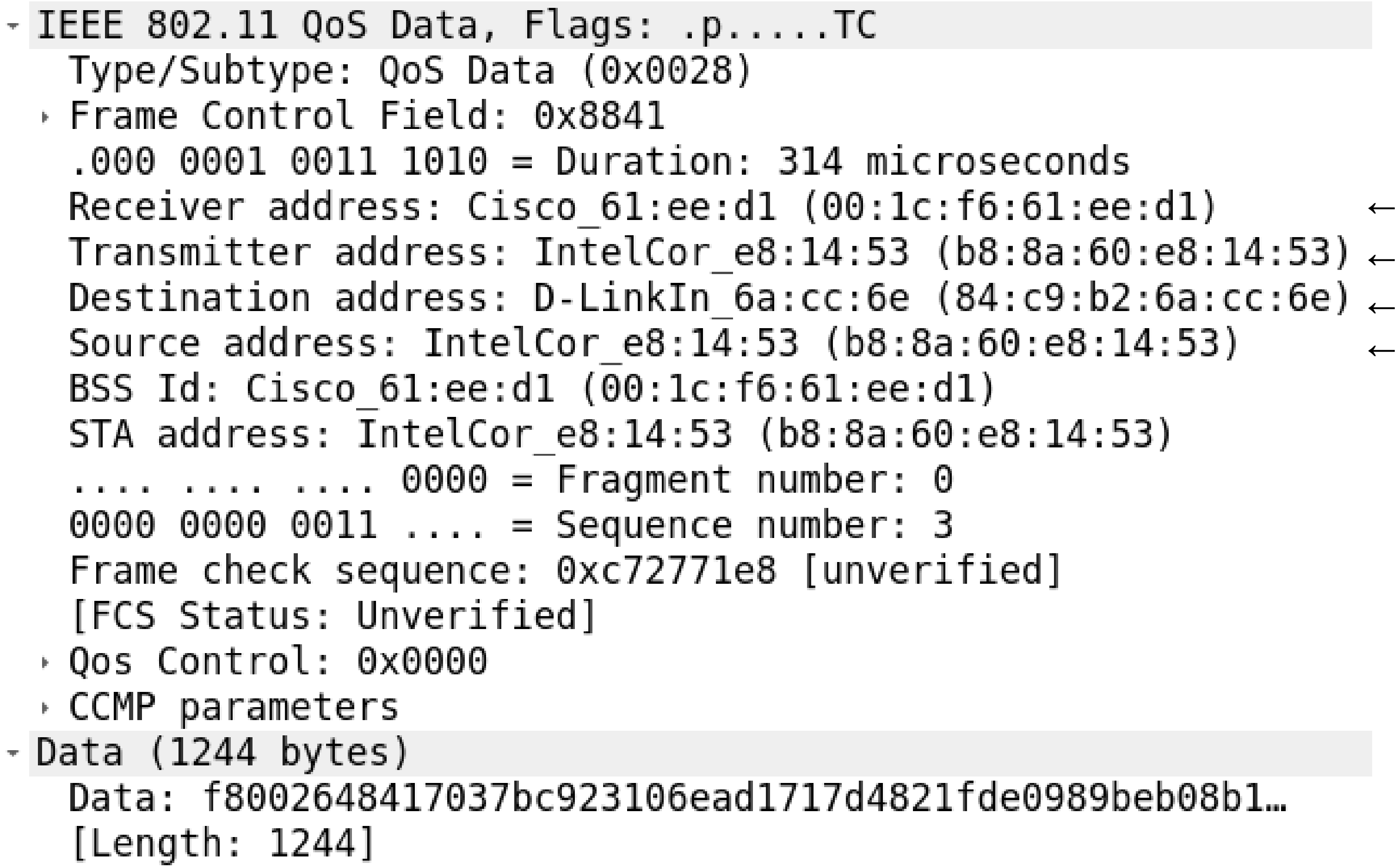
```
▾ IEEE 802.11 Association Request, Flags: ........
    Type/Subtype: Association Request (0x0000)
  ▸ Frame Control Field: 0x0000
    .000 0001 0011 1010 = Duration: 314 microseconds
    Receiver address: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
    Destination address: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
    Transmitter address: D-LinkIn_6a:cc:6e (84:c9:b2:6a:cc:6e)
    Source address: D-LinkIn_6a:cc:6e (84:c9:b2:6a:cc:6e)
    BSS Id: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
    .... .... .... 0000 = Fragment number: 0
    0001 0100 1100 .... = Sequence number: 332
▾ IEEE 802.11 wireless LAN
  ▾ Fixed parameters (4 bytes)
    ▸ Capabilities Information: 0x0421
      Listen Interval: 0x000a
  ▾ Tagged parameters (43 bytes)
    ▸ Tag: SSID parameter set: LABCOM
    ▸ Tag: Supported Rates 1, 2, 5.5, 11, 6, 9, 12, 18, [Mbit/sec]
    ▸ Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]
    ▸ Tag: Extended Capabilities (8 octets)
    ▸ Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Information E
```



```
▾ IEEE 802.11 Association Response, Flags: ........C
    Type/Subtype: Association Response (0x0001)
  ▸ Frame Control Field: 0x1000
    .000 0001 0011 1010 = Duration: 314 microseconds
    Receiver address: D-LinkIn_6a:cc:6e (84:c9:b2:6a:cc:6e)
    Destination address: D-LinkIn_6a:cc:6e (84:c9:b2:6a:cc:6e)
    Transmitter address: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
    Source address: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
    BSS Id: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
    .... .... .... 0000 = Fragment number: 0
    1010 1001 0001 .... = Sequence number: 2705
    Frame check sequence: 0xe7103b15 [unverified]
    [FCS Status: Unverified]
▾ IEEE 802.11 wireless LAN
  ▾ Fixed parameters (6 bytes)
    ▸ Capabilities Information: 0x0421
      Status code: Successful (0x0000)
      ..00 0000 0000 0001 = Association ID: 0x0001
  ▾ Tagged parameters (42 bytes)
    ▸ Tag: Supported Rates 1(B), 2(B), 5.5(B), 6, 9, 11(B), 12, 18, [Mbit/sec]
    ▸ Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]
    ▸ Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
```

From AP →

Data Frame



```
▾ IEEE 802.11 QoS Data, Flags: .p.....TC
    Type/Subtype: QoS Data (0x0028)
  ▸ Frame Control Field: 0x8841
    .000 0001 0011 1010 = Duration: 314 microseconds
    Receiver address: Cisco_61:ee:d1 (00:1c:f6:61:ee:d1)
    Transmitter address: IntelCor_e8:14:53 (b8:8a:60:e8:14:53)
    Destination address: D-LinkIn_6a:cc:6e (84:c9:b2:6a:cc:6e)
    Source address: IntelCor_e8:14:53 (b8:8a:60:e8:14:53)
    BSS Id: Cisco_61:ee:d1 (00:1c:f6:61:ee:d1)
    STA address: IntelCor_e8:14:53 (b8:8a:60:e8:14:53)
    .... .... .... 0000 = Fragment number: 0
    0000 0000 0011 .... = Sequence number: 3
    Frame check sequence: 0xc72771e8 [unverified]
    [FCS Status: Unverified]
  ▸ Qos Control: 0x0000
  ▸ CCMP parameters
▾ Data (1244 bytes)
    Data: f8002648417037bc923106ead1717d4821fde0989beb08b1…
    [Length: 1244]
```

← Node that will receive frame (AP)

← Node that send frame

← Station to receive data

← Station who sent data

- Station “IntelCor*” sending data to station “D-LinkIn*” (via AP).
- Frame captured between station “IntelCor*” and AP (“Cisco*”).

WPA and 802.11i (WPA2)

- **IEEE 802.11i - IEEE 802.11 task group “MAC enhancement for wireless security”.**
- **Wi-Fi Protected Access (WiFi Alliance), WPA, is a subset internal in 802.11i.**
    - Compatible with work developed in 802.11i.
    - Only supports BSS.
    - Defined to work in actual equipment.
        - Firmware update only.
    - Pass-phrase constant and shared, but keys are generated per session.
    - Used in the AP and station.
- WPA has two distinct components.
    - Authentication, based on 802.1X.
    - Ciphering based on TKIP (Temporal Key Integrity Protocol).

WPA

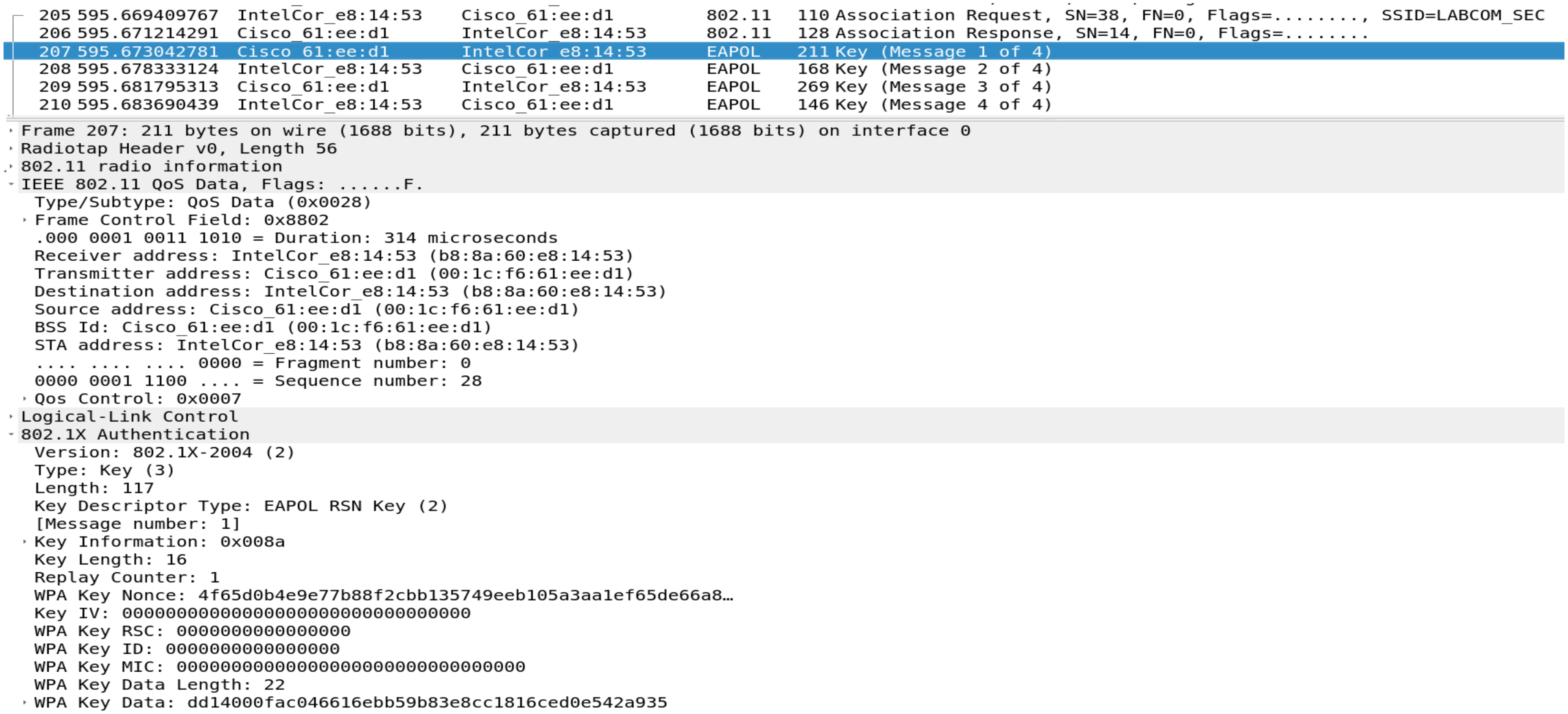
- Authentication
  - 802.1X (≠ 802.11x) – defined for wired and wireless sessions, as a transport protocol
    - EAP (Extensible Authentication Protocol) – like a wrapper for the specific authentication traffic
    - Impact of EAP
      - Authentication does not traverse the AP (STA - server)
      - It is possible to use different authentication methods without changing APs
  - Defines also a Pre-Shared Key (PSK)
    - For local networks
- Temporal Key Integrity Protocol (TKIP) – internal solution with better protection, for actual equipments
  - Greater privacy
    - Uses the same cipher, but now associated to the MAC and a larger IV
    - “Key rollover” with temporal validity
  - Greater integrity
    - Integrity separated key

802.11i (WPA2)

- Better than WPA
  - Also includes TKIP
  - Authentication IBSS (ad-hoc mode)?
  - RSN (Robust Security Network) protocol
    - Authentication and ciphering between APs and stations
    - Supports new ciphering protocols, resorting to 802.1x and EAP
    - Supports AES (Advanced Encryption Standard) ciphering
- Problems
  - It does not cipher control and management frames
    - (Disassociate, output power, etc).
  - Requires new hardware

WPA* Key Exchange (EAP phase 2)

- Done during the Association process.
  - After Association Request/response frames.
  - Uses (QoS) Data Frames

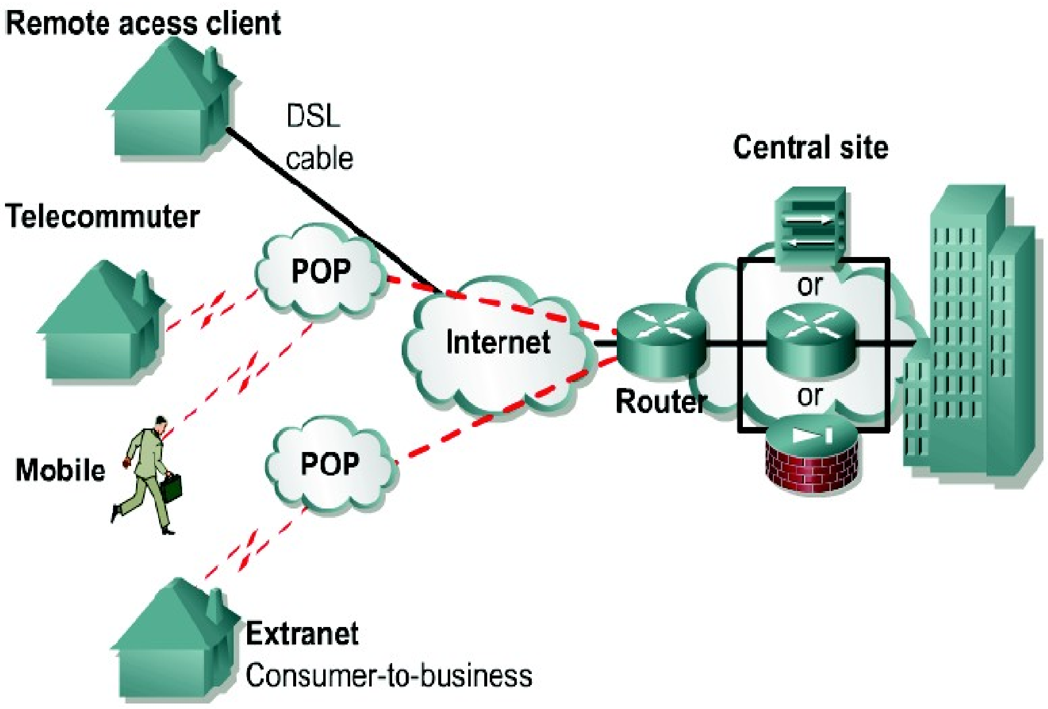


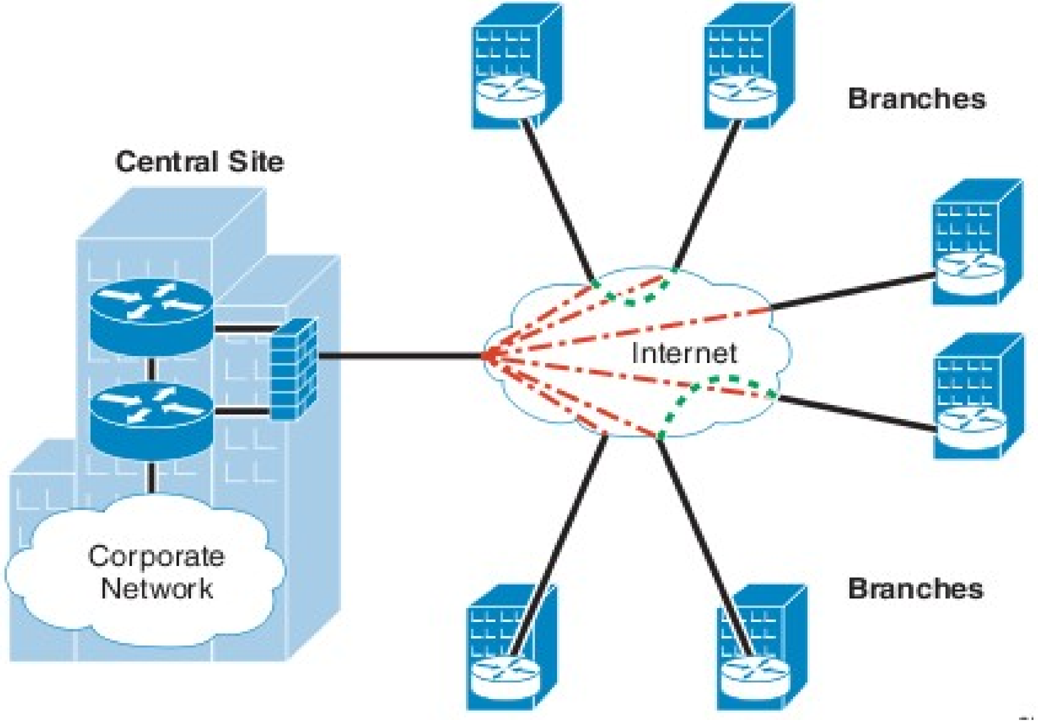
```
205 595.669409767  IntelCor_e8:14:53   Cisco_61:ee:d1      802.11   110 Association Request, SN=38, FN=0, Flags=........, SSID=LABCOM_SEC
206 595.671214291  Cisco_61:ee:d1      IntelCor_e8:14:53   802.11   128 Association Response, SN=14, FN=0, Flags=........
207 595.673042781  Cisco_61:ee:d1      IntelCor_e8:14:53   EAPOL    211 Key (Message 1 of 4)
208 595.678333124  IntelCor_e8:14:53   Cisco_61:ee:d1      EAPOL    168 Key (Message 2 of 4)
209 595.681795313  Cisco_61:ee:d1      IntelCor_e8:14:53   EAPOL    269 Key (Message 3 of 4)
210 595.683690439  IntelCor_e8:14:53   Cisco_61:ee:d1      EAPOL    146 Key (Message 4 of 4)

Frame 207: 211 bytes on wire (1688 bits), 211 bytes captured (1688 bits) on interface 0
Radiotap Header v0, Length 56
802.11 radio information
IEEE 802.11 QoS Data, Flags: ......F.
  Type/Subtype: QoS Data (0x0028)
  Frame Control Field: 0x8802
  .000 0001 0011 1010 = Duration: 314 microseconds
  Receiver address: IntelCor_e8:14:53 (b8:8a:60:e8:14:53)
  Transmitter address: Cisco_61:ee:d1 (00:1c:f6:61:ee:d1)
  Destination address: IntelCor_e8:14:53 (b8:8a:60:e8:14:53)
  Source address: Cisco_61:ee:d1 (00:1c:f6:61:ee:d1)
  BSS Id: Cisco_61:ee:d1 (00:1c:f6:61:ee:d1)
  STA address: IntelCor_e8:14:53 (b8:8a:60:e8:14:53)
  .... .... .... 0000 = Fragment number: 0
  0000 0001 1100 .... = Sequence number: 28
  Qos Control: 0x0007
Logical-Link Control
802.1X Authentication
  Version: 802.1X-2004 (2)
  Type: Key (3)
  Length: 117
  Key Descriptor Type: EAPOL RSN Key (2)
  [Message number: 1]
  Key Information: 0x008a
  Key Length: 16
  Replay Counter: 1
  WPA Key Nonce: 4f65d0b4e9e77b88f2cbb135749eeb105a3aa1ef65de66a8…
  Key IV: 00000000000000000000000000000000
  WPA Key RSC: 0000000000000000
  WPA Key ID: 0000000000000000
  WPA Key MIC: 00000000000000000000000000000000
  WPA Key Data Length: 22
  WPA Key Data: dd14000fac046616ebb59b83e8cc1816ced0e542a935
```

Virtual Private Networks (VPN)

VPN - Virtual Private Networks

- Is an encrypted connection between private networks over a public network





- Remote Access VPN
- Site-to-Site VPN

VPN types

- Remote Access VPN
  - PPTP
  - L2TP/IPsec
  - SSL/TLS VPN
    - Web VPN (client-less SSL VPN) – VPN client can be a standard browser
  - SSH VPN
  - Open VPN
- Site-to-Site VPN
  - IPsec VPN
    - With static or dynamic configuration
  - IPsec + GRE VPN
    - Dynamic Multipoint VPN

Remote Access VPN - PPTP VPN

- Based on PPTP
  - PPTP packages data within PPP packets
  - Encapsulates the PPP packets within IP packets
- Uses a form of General Routing Encapsulation (GRE) to get data to and from its final destination
- Supports authentication based on protocols PAP, EAP, CHAP, MS-CHAPv1 and MS-CHAPv2
- Uses MPPE as cipher
  - Has two different keys (one for each direction)
  - Requires MS-CHAPv2 authentication
  - Keys derived from the MS-CHAPv2's password hash and challenges
- PPTP creates a TCP control connection between the VPN client and VPN server to establish a tunnel
  - Uses TCP port 1723 for these connections
- PPTP can support only one tunnel at a time for each user

Remote Access VPN - L2TP/IPSec VPN

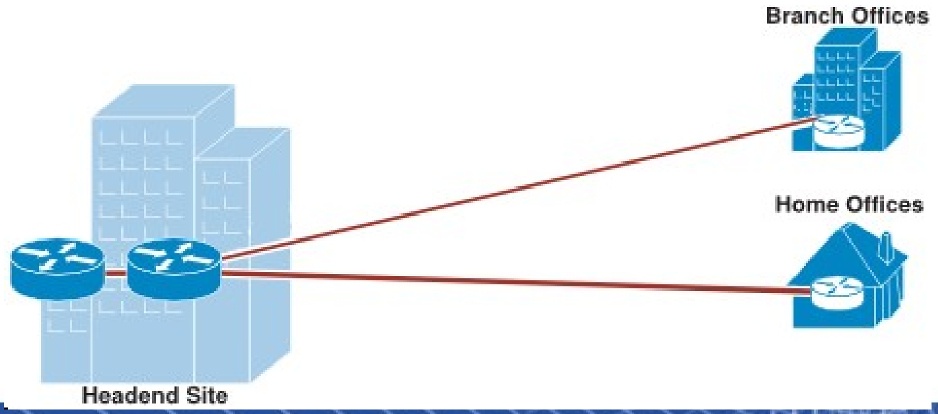
- Authentication can be performed with Digital Certificates (RSA) or with the same PPP authentication mechanisms as PPTP
- Provides data integrity, authentication of origin and replay protection
- Encryption provided by IPSec (ESP protocol)
- Can support multiple, simultaneous tunnels for each user
- Slower performance than PPTP

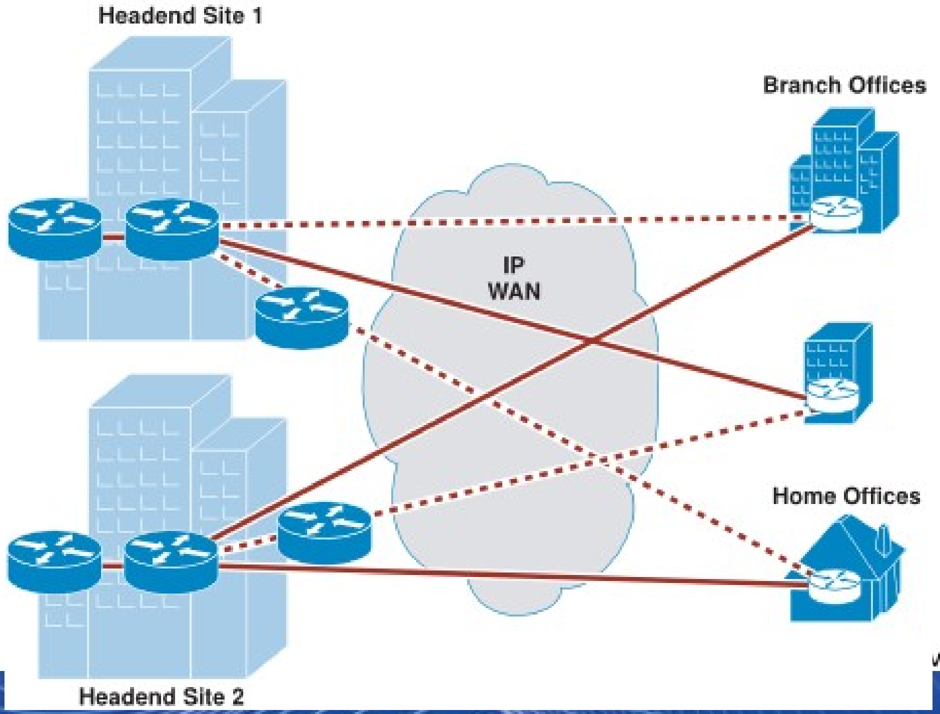
Other Remote Access VPN types

- SSL/TLS VPN
  - SSL/TLS protocol handles the VPN tunnel creation
  - SSL/TLS is much easier to implement than IPSec and provides a simple and well-tested platform
  - RSA handshake (or DH) is used exactly as IKE in IPSec
- SSH VPN
  - VPN over a SSH connection
  - SSH tunneling - port forwarding
- OpenVPN
  - Implements a SSL/TLS VPN
  - Allows PSK, certicate, and login/password based authentication
  - Encryption provided by OpenSSL (can use all ciphers available)
  - Compatible with dynamic and NAT addresses

Variants of Site-to-Site IPsec VPN

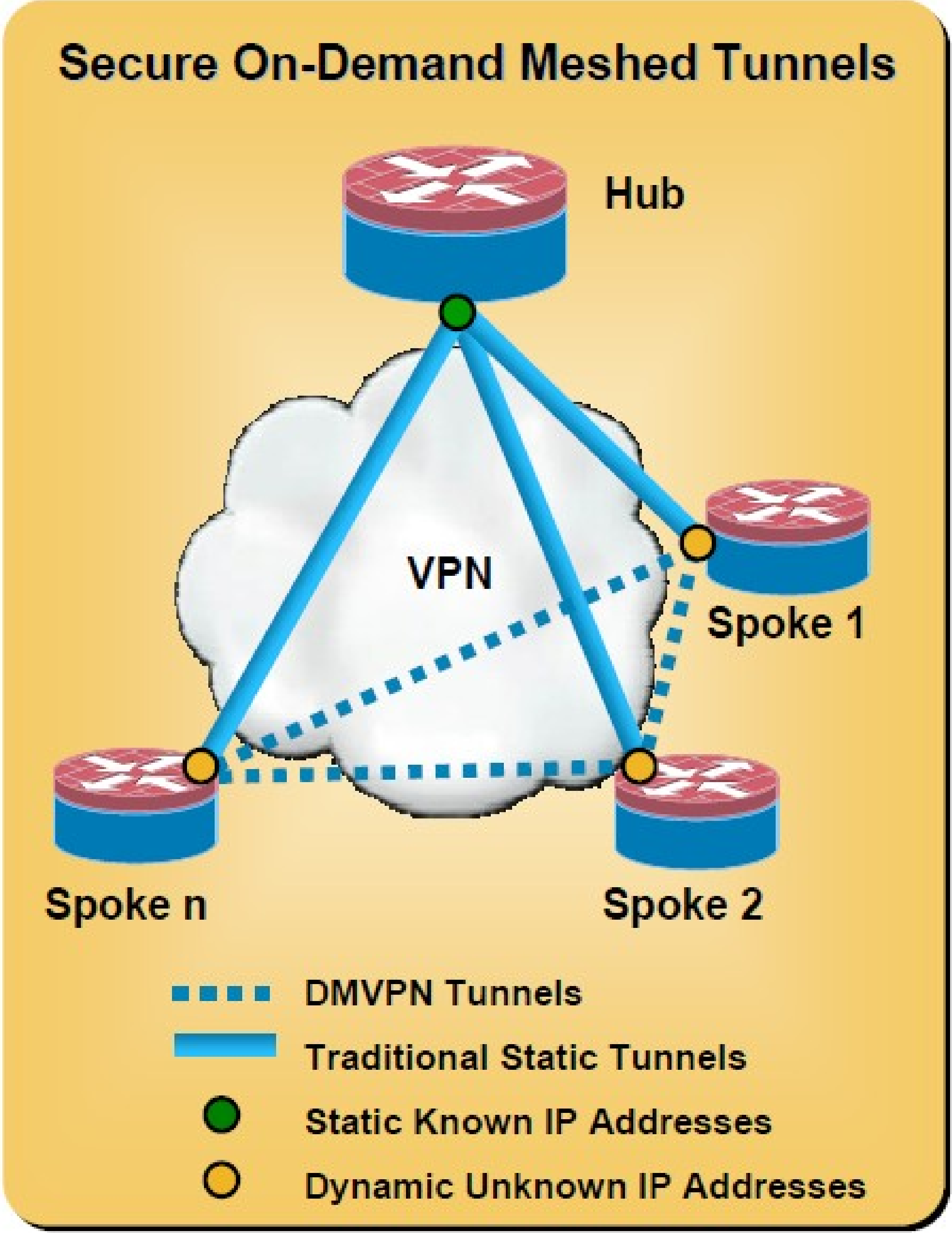
- IPsec tunnels with static configuration
  - Requires the knowledge of all peers (IP addresses and security parameters)
  - High configuration overhead
- IPsec tunnels with dynamic configuration (at the headend/hub)
  - Hub + spokes configuration
  - Generic configuration at the headend/hub
  - Easy to add new spokes
- ➔ A basic IPsec tunnel can't protect multicast traffic.
- IPsec + GRE tunnels
  - Generic Routing Encapsulation (GRE) allows the protection of multicast traffic over IPsec
- Dynamic Multipoint VPN (DMVPN)



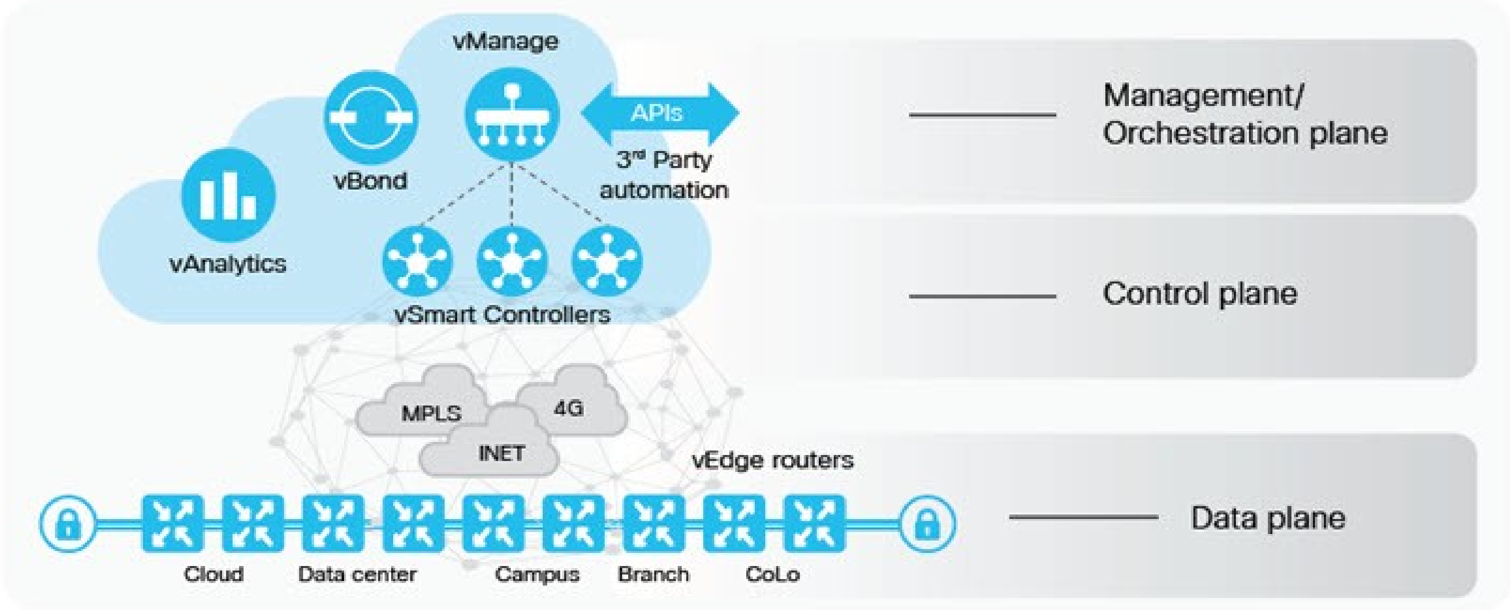


Dynamic Multipoint VPN

- Provides full meshed connectivity with simple configuration of hub and spoke
- Supports dynamically addressed spokes
- Facilitates zero-touch configuration for addition of new spokes
- Features automatic IPsec triggering for building an IPsec tunnel


Secure On-Demand Meshed Tunnels
Hub
VPN
Spoke 1
Spoke n
Spoke 2
DMVPN Tunnels
Traditional Static Tunnels
Static Known IP Addresses
Dynamic Unknown IP Addresses

SD-WAN



- Software Defined WAN
  - Edge Connectivity Abstraction.
  - WAN Virtualization.
  - Policy-Driven, Centralized Management.
  - Elastic Traffic Management.
  - Advantages: Easy deployment and management.
  - Disadvantages: Completely dependence (present and future) on external providers.

Network Security Systems

Network Security Systems

- Firewall
- Intrusion Prevention System (IPS)
  - Performs deep-packet inspection
- Intrusion Detection Systems (IDS)
  - Performs deep-packet (DPI) and shallow-packet inspection (SPI)
- Security Appliance
  - Unified communications security
  - Firewall services
  - Real-time threat defense
  - Secure remote access
  - Secure communications services
  - Content security

Firewalls

- A firewall provides a single point of defense between networks and protects one network from the others-
- It is a system or group of systems that enforces a control policy between two or more networks (access control, flow control and content control).
- It is a network gateway that enforces the rules of network security.
- Minimizes local vulnerabilities.
- Evaluates each network packet against the policies of network security.
- Can monitor all the network traffic and alert to any attempts to bypass security or to any patterns of inappropriate use.
- Can be hardware or software based.

Firewalls Security/Network Services

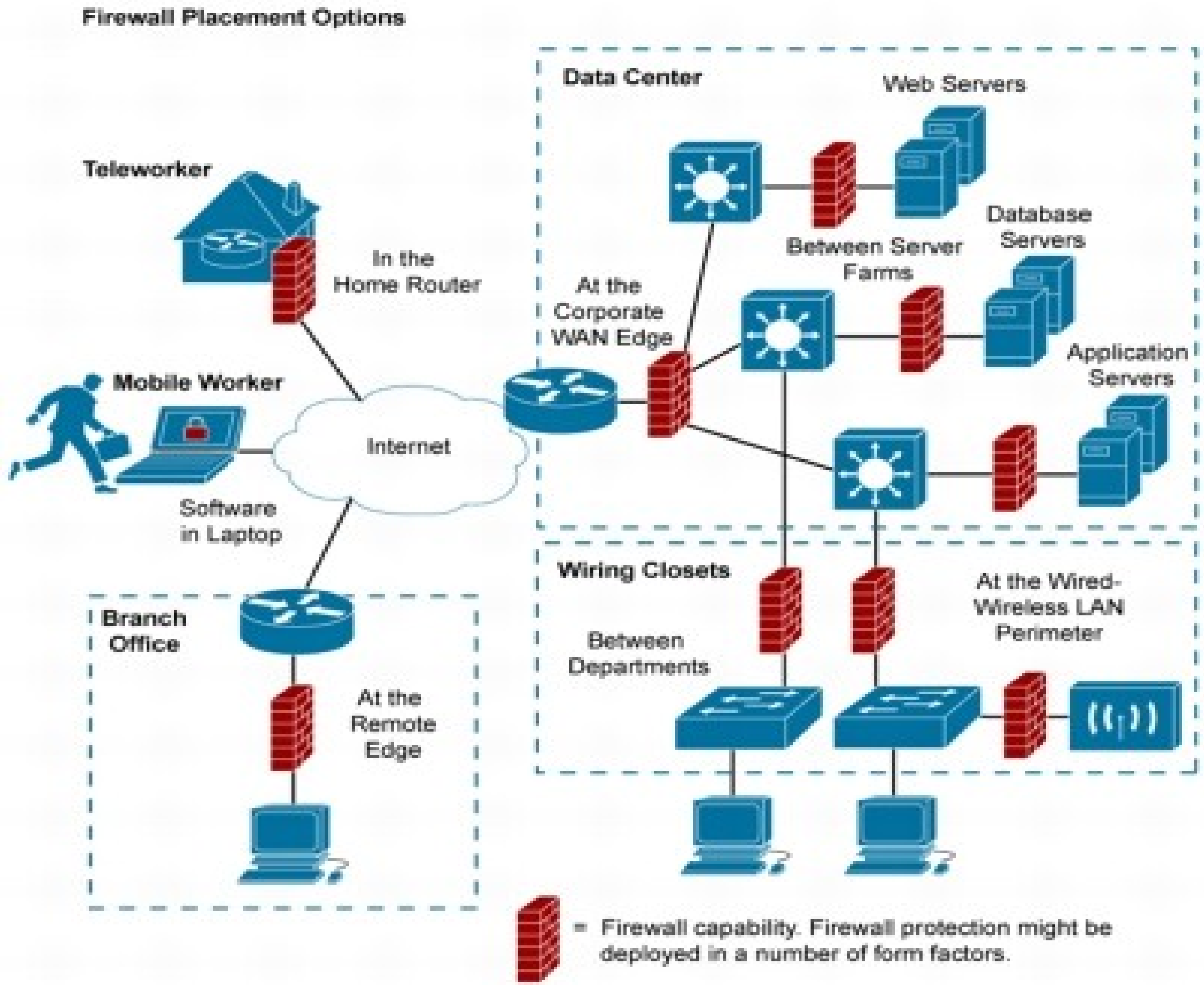
- NAT (Network Address Translation).
- Authorization
  - Flows (packet filtering).
  - Users (application and circuit level).
- Redirecting.
  - To specif machines.
  - Proxing.
- Content analysis.
- Secure communication.
  - Site-to-site VPN.
    - IPsec.
  - Remote-access VPN.
- DoS and DDoS detection and defense.

Types of Firewalls

- Network-Level Firewalls (L2/L3)
  - Packet filtering
  - Inspecting packet headers and filtering traffic based on
    - the IP address of the source and the destination, the port and the service (L3)
    - source and the destination MAC addresses (L2)
- Circuit-Level Firewalls (L4)
  - Monitor TCP handshaking between packets to make sure a session is legitimate
  - Traffic is filtered based on specified session rules
- Application-Level Firewalls (L4+)
  - Application-level firewalls are sometimes called proxies
  - Looking more deeply into the application data
  - Consider the context of client requests and application responses
  - Attempt to enforce correct application behavior and block malicious activity
  - Application-level filtering may include protection against Spam and viruses as well, and block undesirable Web sites based on content rather than just their IP address
  - Slow and resources consuming tasks
- Stateful Multi-level Firewalls (L*)
  - Filter packets at the network level and they recognize and process application-level data
  - Since they don't employ proxies, they have reasonably good performance even performing deep packet analysis
- Host Level / Personal Firewalls
  - Act only within a specif host
  - Filter all communication layers
  - Control OS processes/applications

Deploying Firewalls

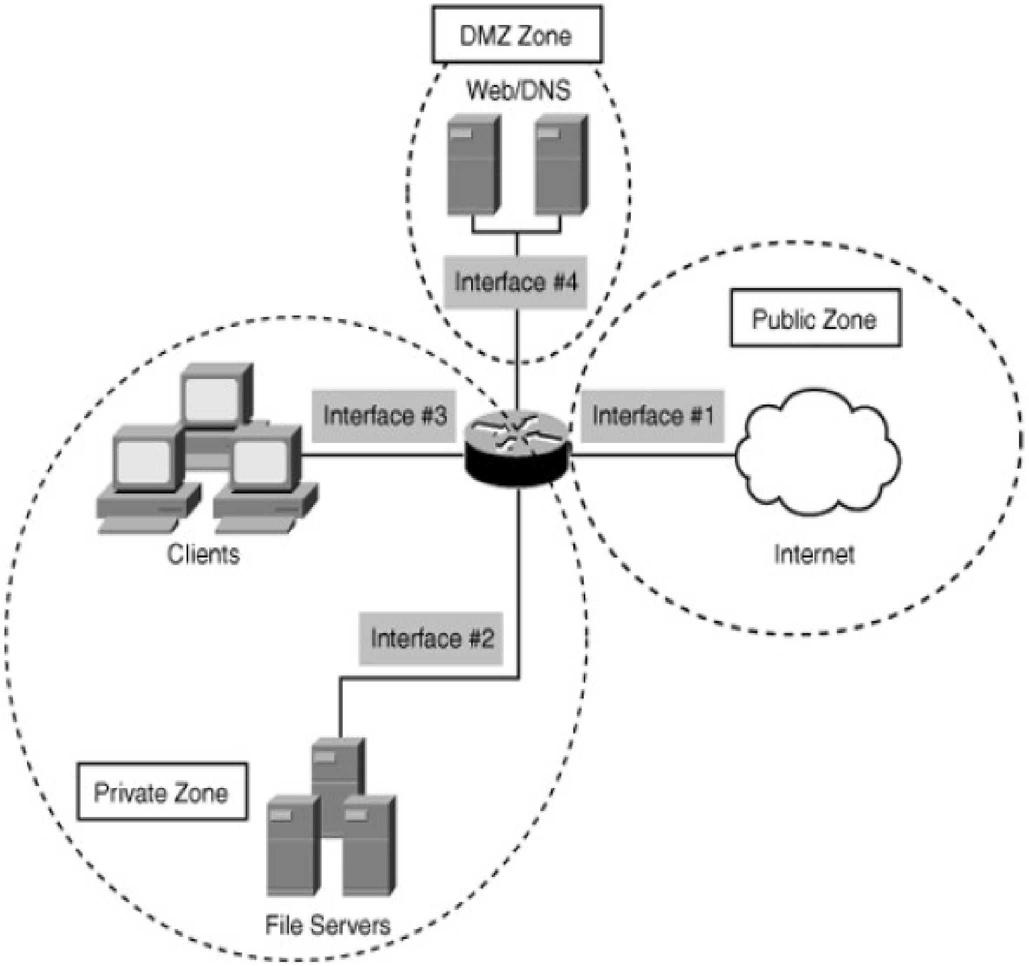
- Network must be protected at multiple levels and locations



Stateful vs. Stateless Firewalls

- Stateless firewalls
  - Controls traffic by applying rules to single frames/packets
    - Does not need to track traffic flows/sessions.
  - Rules based on specific values on frames/packet available headers.
    - Set of basic permit/deny actions for input and output based on IP addresses, UDP/TCP ports, etc…
    - Usually called ACL (Access List).
  - They are fast and consume very low computing resources.
    - Perform well under heavy traffic load.
    - Ideal to defense against DDoS attacks in the first line of network defense.
    - Cost-effective compared with stateful firewall types.
- Stateful firewalls
  - Monitor all traffic flows/sessions.
  - Controls traffic based on the connection state of a flow/session.
    - Automatic bidirectional rules (reflexive rules).
  - Connection state is maintained in a state table.
    - State tables must be synchronized with other firewalls when in a redundant scenario (load balancing) or high-availability scenario (backup upon failure).

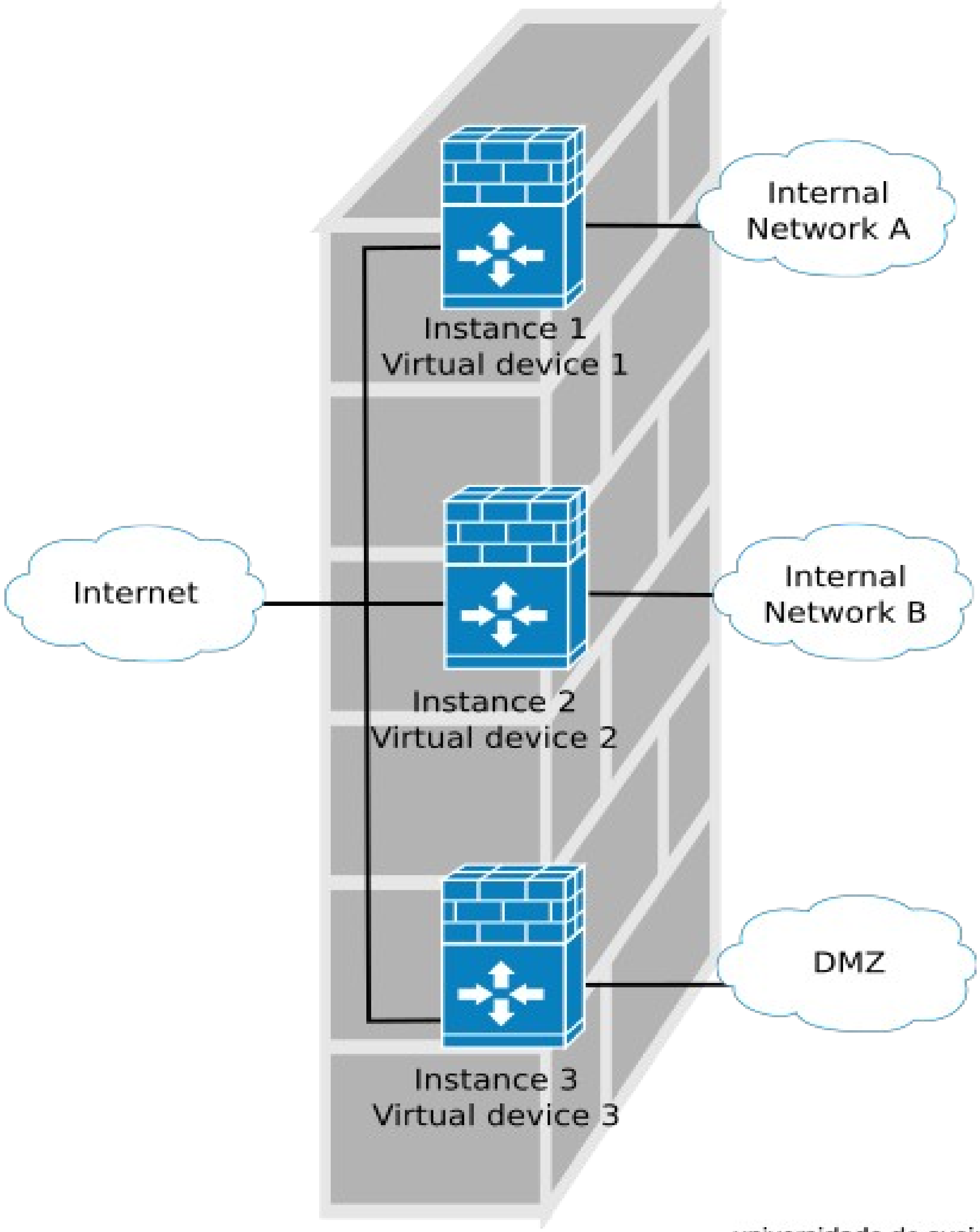
Firewall Zones/Group



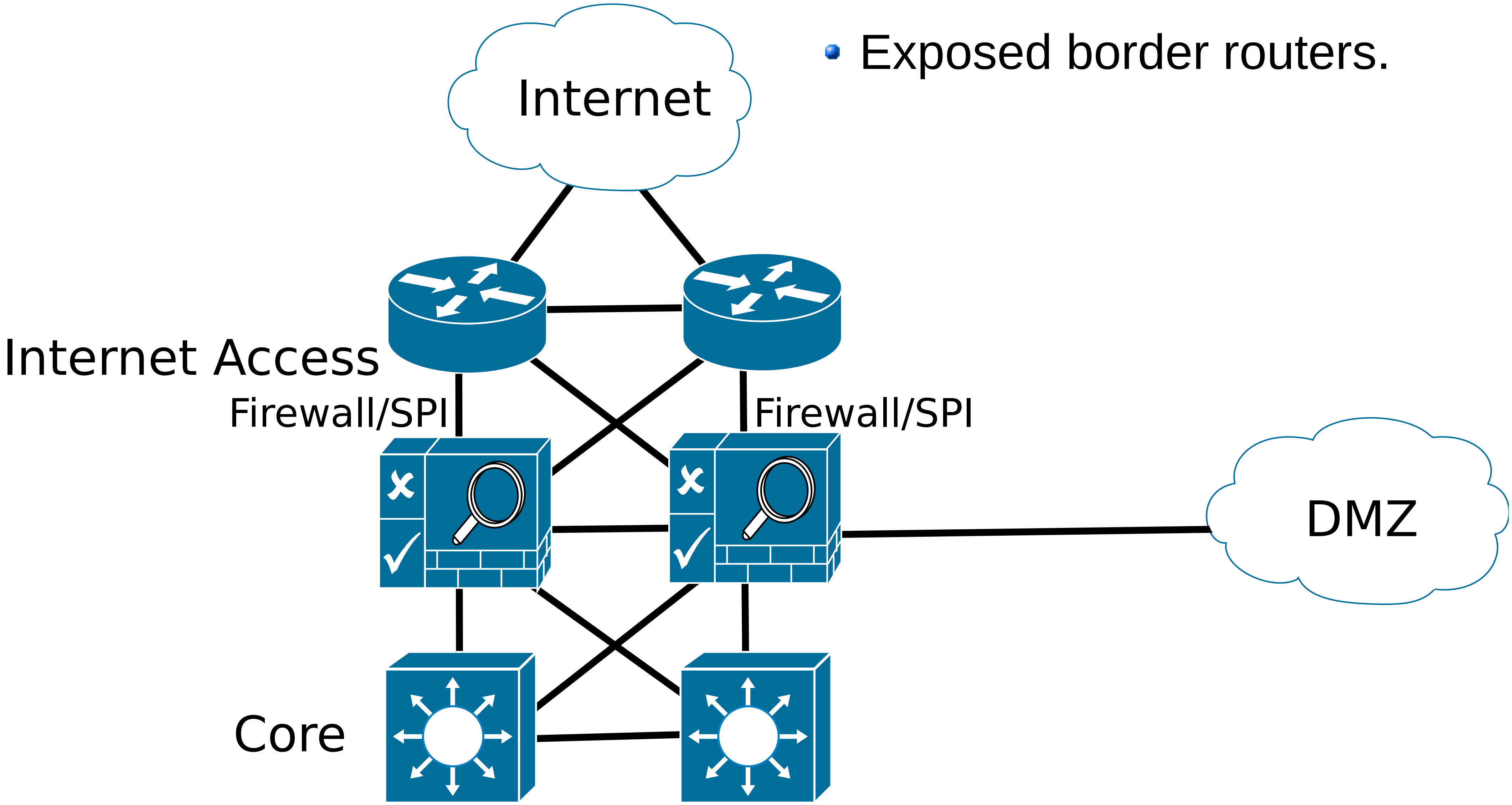
- A network can be divided in multiple zones/groups with different security levels.
  - Collections of IP addresses, networks, or ports.
- Once created, a group can be referenced by firewall rules as either a source or destination.
- Example: a Demilitarized Zone (DMZ) is a perimeter network outside the protected internal/private network
  - Used to place public servers/services.
  - The DMZ is a "semi-protected" Zone.
    - It must be assumed that any machine placed on the DMZ is at risk.

Firewall Virtual Instances

- Firewalls may have (theoretical) isolated instances to handle different zones/groups.
- Each instance is a virtual device that can perform flow control, switch, and/or routing.

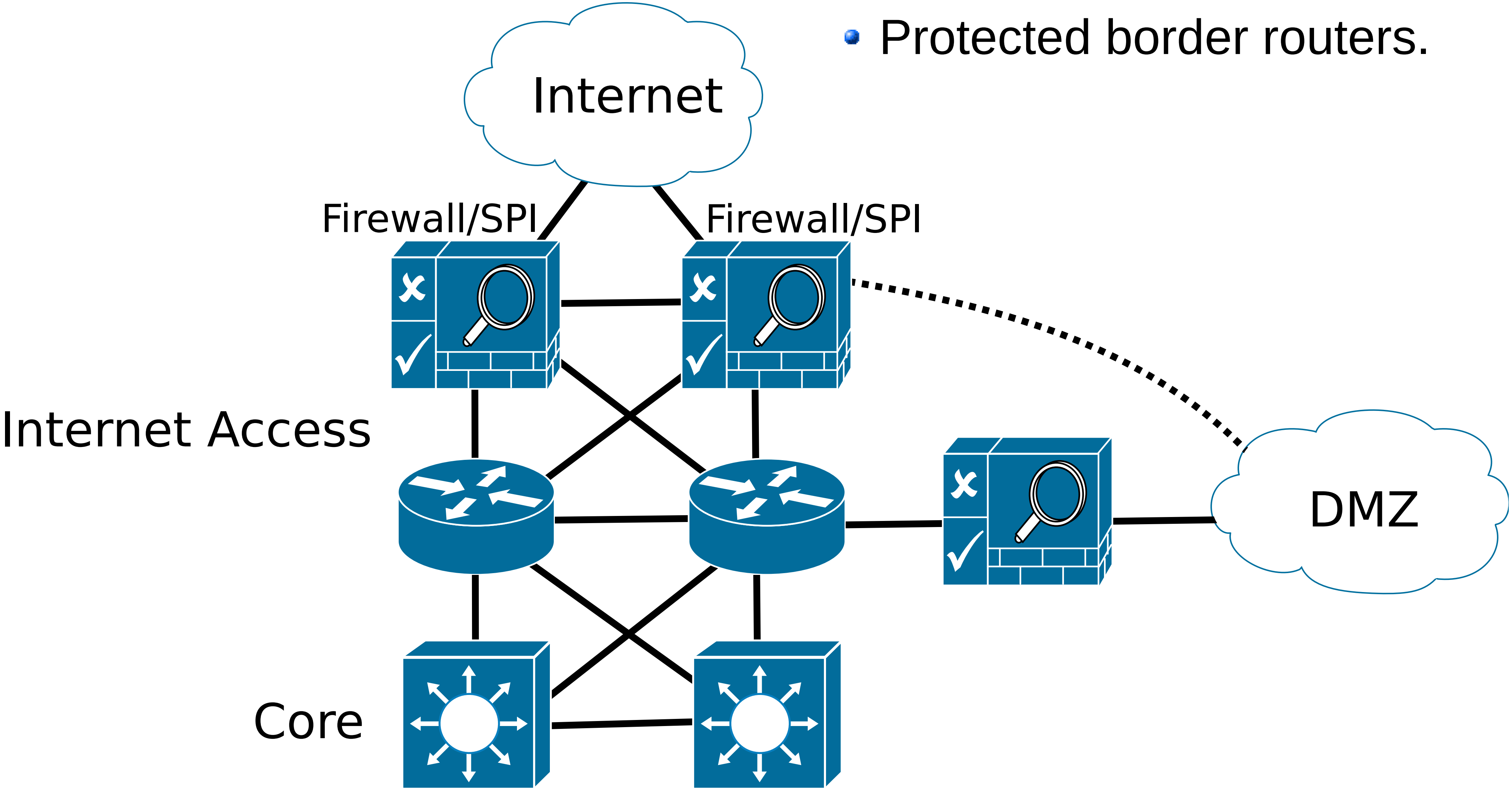

Internal Network A
Instance 1 Virtual device 1
Internet
Internal Network B
Instance 2 Virtual device 2
DMZ
Instance 3 Virtual device 3

Firewall placement (with Redundancy)



- Exposed border routers.

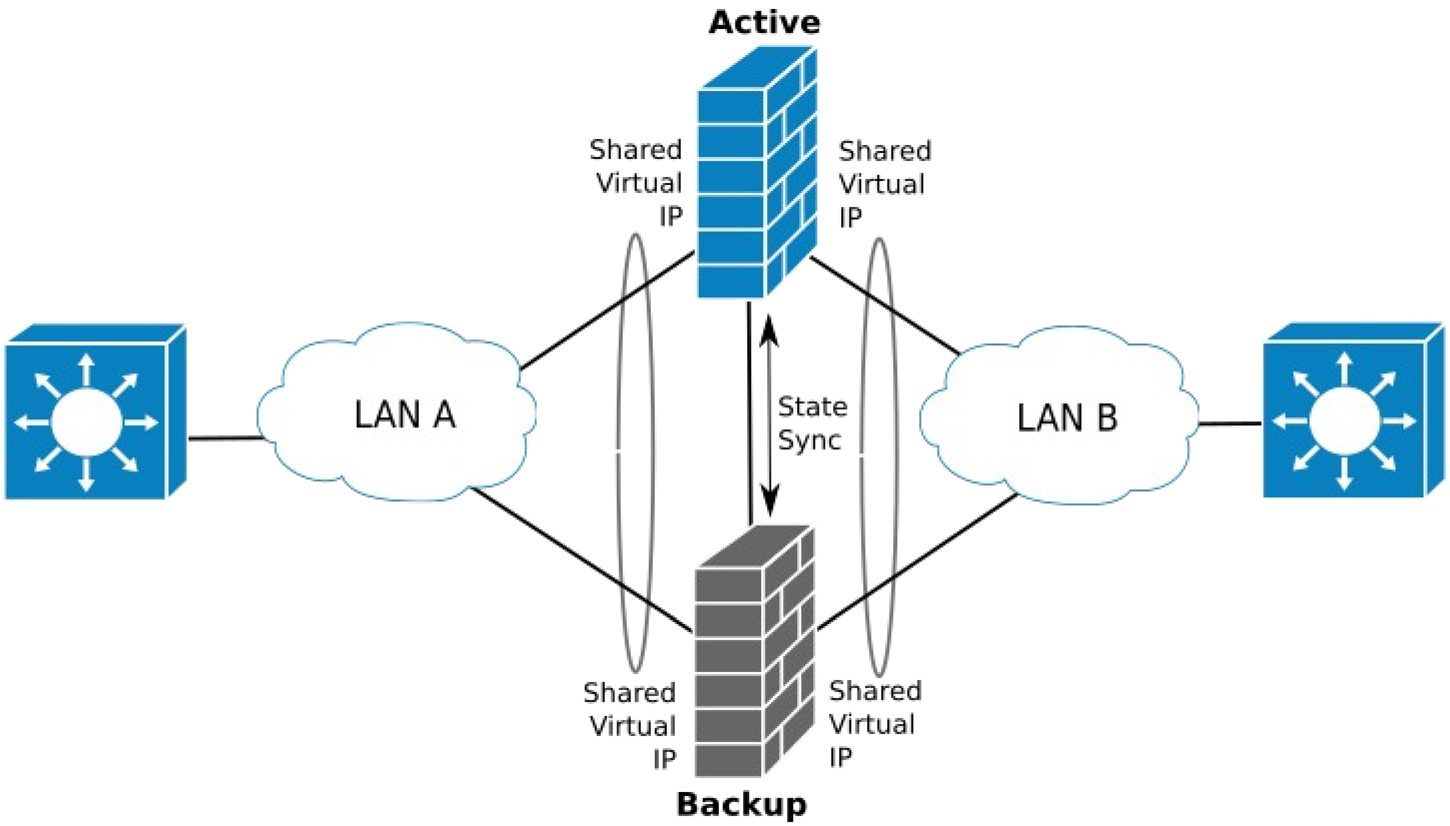
Firewall placement (with Redundancy)



- Protected border routers.

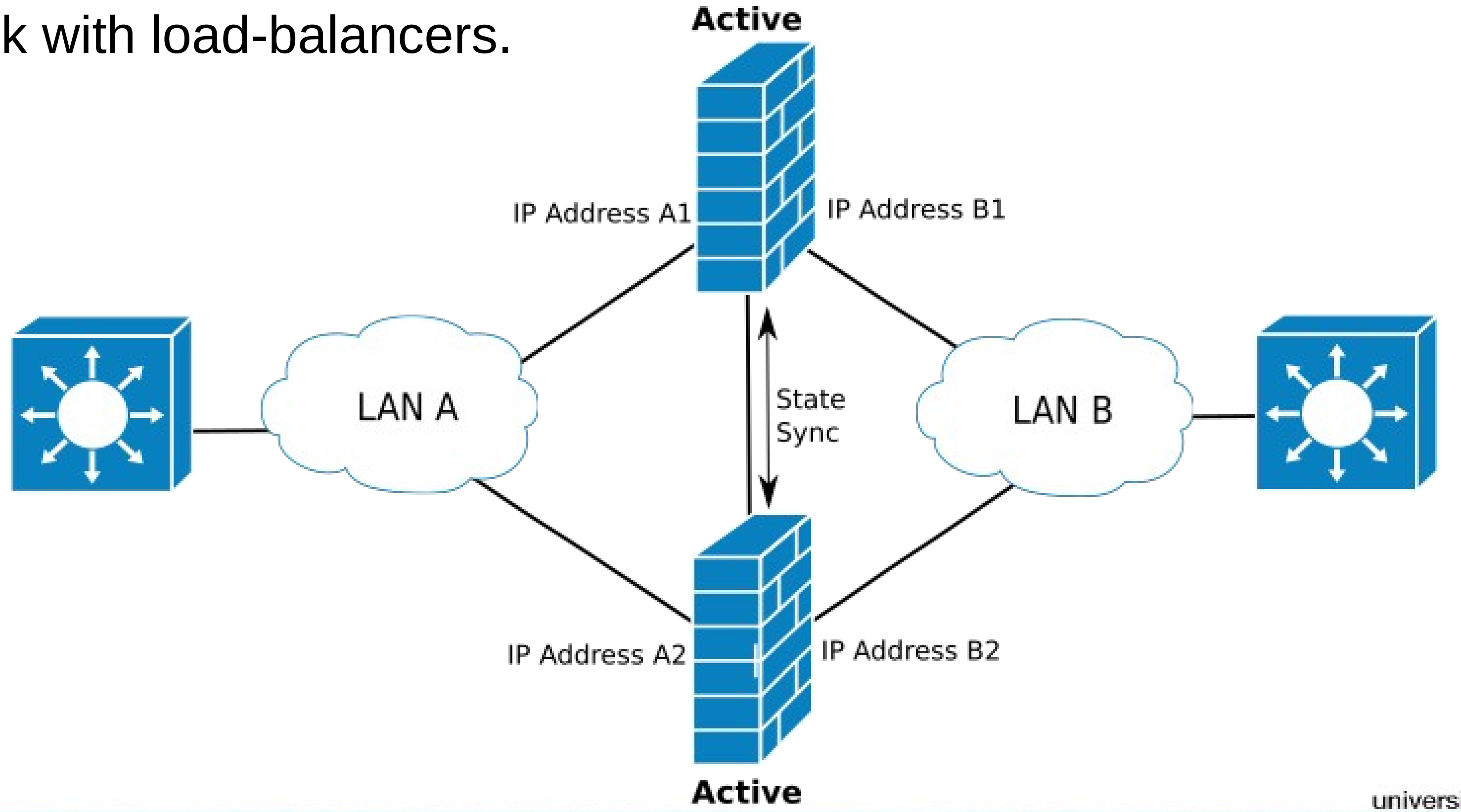
High-Availability (1)

- Active-Backup Scenario
  - Firewalls share state via a dedicated connection
  - Firewalls share LAN (Virtual) IP addresses.
  - Backup firewall assumes IP and Services upon failure of Active firewall.



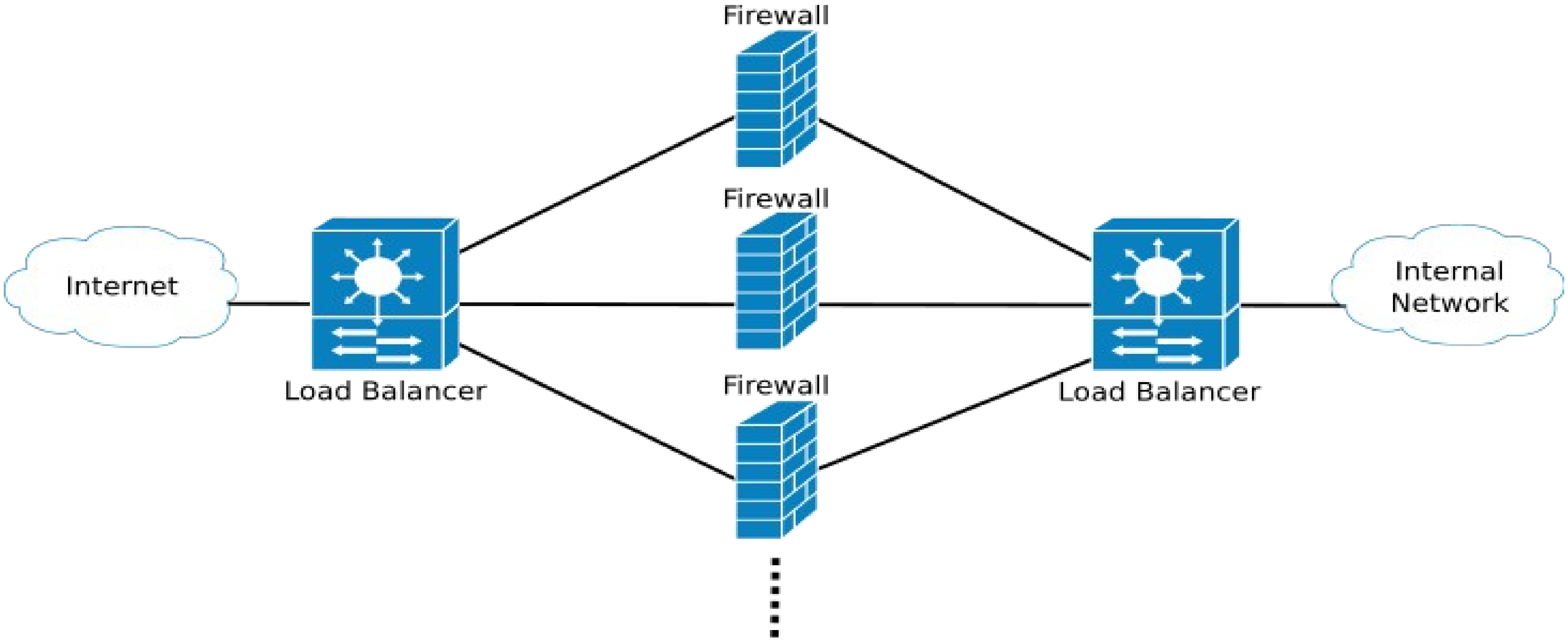
High-Availability (2)

- Active-Active Scenario
  - Firewalls share state via a dedicated connection
  - Firewalls have their on IP addresses.
  - Both work simultaneously.
    - Share load.
    - Solve asymmetric routing problem.
    - Work with load-balancers.



Load Balancing Firewall Load

- Load-balancing equipment can distribute traffic by multiple firewalls.
  - Decrease processing and memory requirements of each firewall.
  - Allow for a scalable growth of traffic.
  - Makes the network less vulnerable to DoS attacks.
  - When its also responsible to distribute policies/rules is called an Orchestrator.

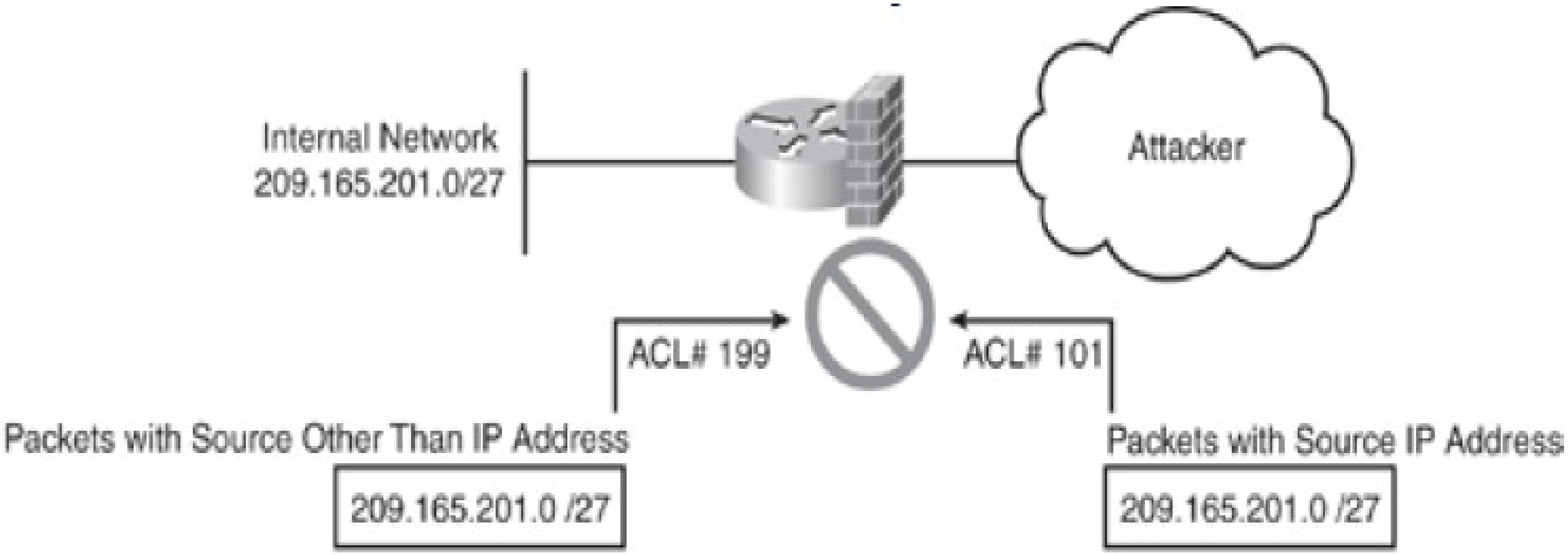


Load Balancing Algorithms

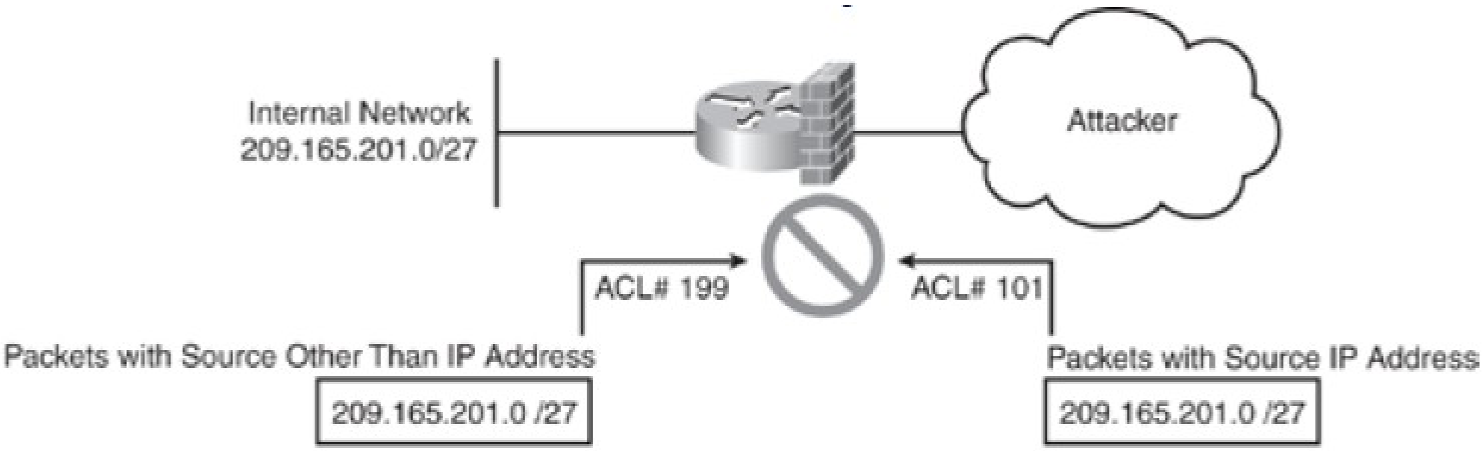
- IP Hash
  - The IP address (or a set of flow identifiers) of the client is used to determine which server/firewall receives the flow or request.
  - Does not require state maintenance. Hash function output determines target.
- Round Robin
  - Requests are distributed across the group of servers sequentially.
  - Can not be used with firewalls, if firewalls do not share state.
- Least Connections
  - A new request is sent to the server/firewall with the fewest current connections.
  - The relative computing capacity of each server/firewall is factored into determining which one has the least connections.
- “Smart”
  - Based on an external source of information.

IP Spoofing

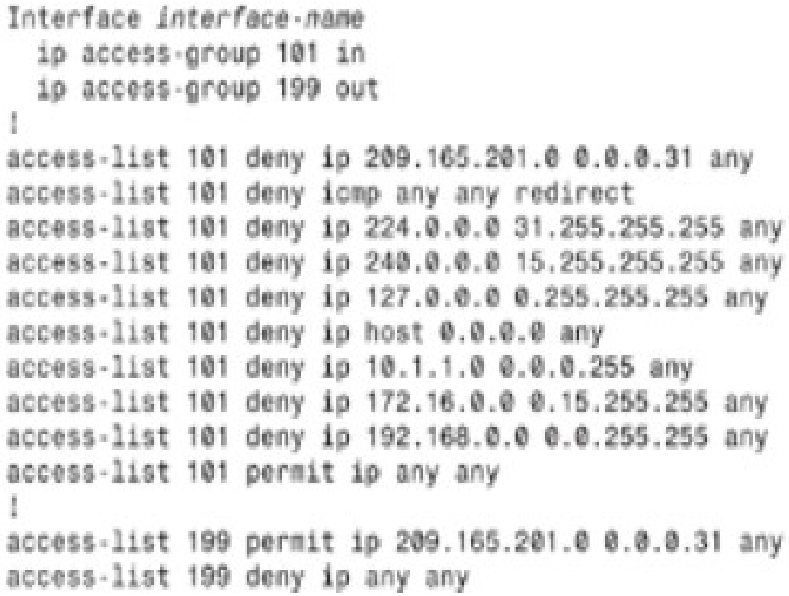
- IP spoofing refers to the creation of IP packets with a forged source IP address.
  - To hide the identity of the sender or impersonate another network system.
  - Spoofing IP datagrams is a well-known problem.
  - Most spoofing is done for illegitimate purposes.



Preventing IP Spoofing at Layer 3

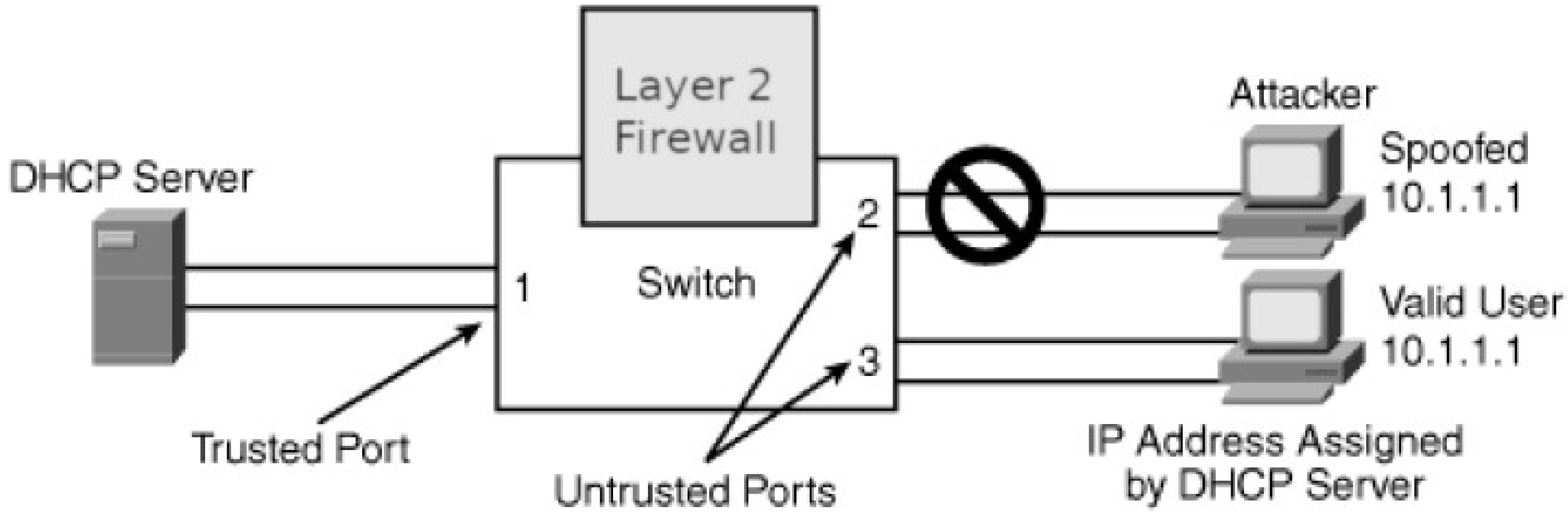


- Deny external traffic with
  - IP source equal to protected network IP ranges.
  - IP source equal to private addresses.
  - Multicast destinations.
- Reverse Path Verification
  - Deny traffic where the source IP network is not reachable using the interface where the packet arrived.



```
Interface interface-name
  ip access-group 101 in
  ip access-group 199 out
!
access-list 101 deny ip 209.165.201.0 0.0.0.31 any
access-list 101 deny icmp any any redirect
access-list 101 deny ip 224.0.0.0 31.255.255.255 any
access-list 101 deny ip 240.0.0.0 15.255.255.255 any
access-list 101 deny ip 127.0.0.0 0.255.255.255 any
access-list 101 deny ip host 0.0.0.0 any
access-list 101 deny ip 10.1.1.0 0.0.0.255 any
access-list 101 deny ip 172.16.0.0 0.15.255.255 any
access-list 101 deny ip 192.168.0.0 0.0.255.255 any
access-list 101 permit ip any any
!
access-list 199 permit ip 209.165.201.0 0.0.0.31 any
access-list 199 deny ip any any
```

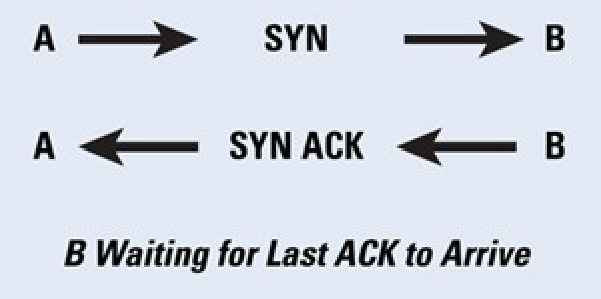
Preventing IP Spoofing at Layer 2



- To prevent IP spoofing attacks by restricting IP traffic on untrusted Layer 2 ports to clients with an assigned IP address.
- Works by filtering IP traffic with a source IP address other than that assigned via Dynamic Host Configuration Protocol (DHCP) or static configuration on the untrusted Layer 2 ports.
- Works in combination with the DHCP and is enabled on untrusted Layer 2 ports.

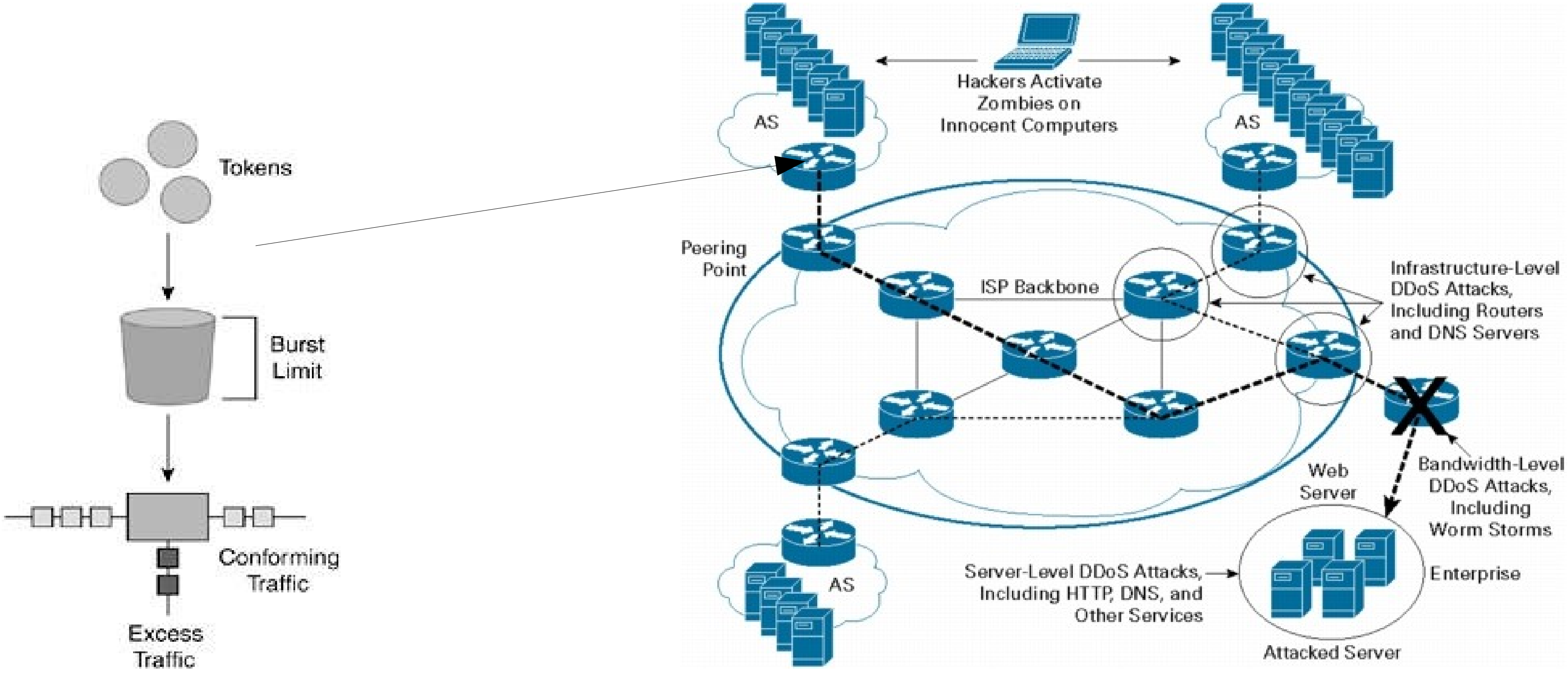
Half-Open TCP Connection Problem

- A DoS attack commonly uses half-open TCP connections.
  - Firewall keeps the state of the TCP session in memory.
  - Multiple half-open TCP connections can overrun firewalls.
    - Define timeout values for half-open TCP sessions:
      - Normal: small/medium values.
      - Under attack (based on traffic thresholds): very small values.
    - May be necessary to use external means to “clean” firewall.
      - Reseting (half-open) connections from the internal servers.



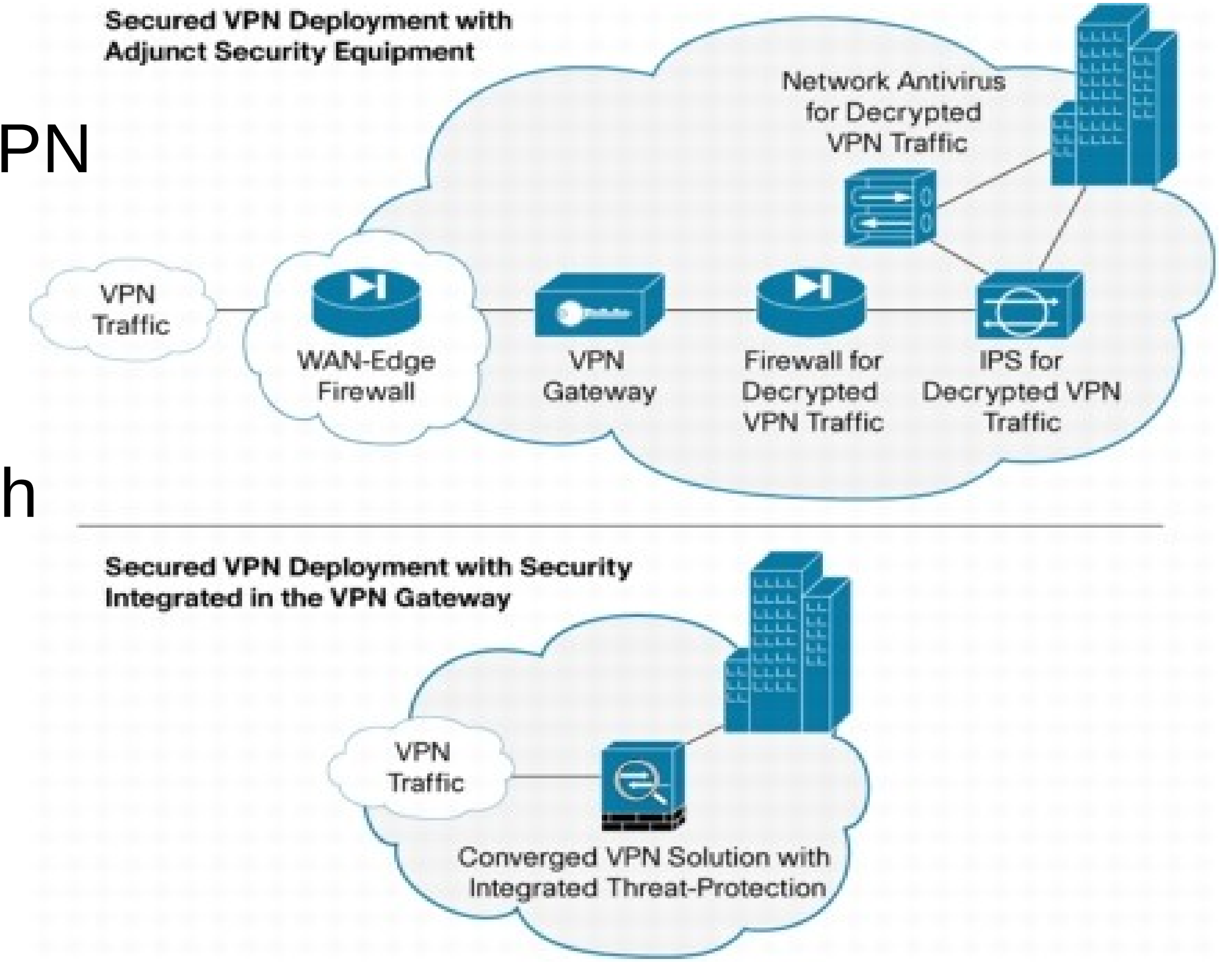
DDoS Mitigation at Source

- CAR - Committed Access Rate
  - Limits (a class of traffic) traffic to a specific rate
  - Token bucket model
  - Avoids that a single source may generate/transmit traffic above a per-defined threshold


Tokens
Burst Limit
Conforming Traffic
Excess Traffic
Hackers Activate Zombies on Innocent Computers
AS
AS
Peering Point
ISP Backbone
Infrastructure-Level DDoS Attacks, Including Routers and DNS Servers
Bandwidth-Level DDoS Attacks, Including Worm Storms
Web Server
AS
Server-Level DDoS Attacks, Including HTTP, DNS, and Other Services
Enterprise
Attacked Server

Firewalls and Remote-Access VPN

- Firewalls need work with VPN gateways
  - To filter all traffic
  - To filter decrypt VPN traffic
- Most firewalls integrate both Security and VPN gateway services


Secured VPN Deployment with Adjunct Security Equipment
Network Antivirus for Decrypted VPN Traffic
VPN Traffic
WAN-Edge Firewall
VPN Gateway
Firewall for Decrypted VPN Traffic
IPS for Decrypted VPN Traffic
Secured VPN Deployment with Security Integrated in the VPN Gateway
VPN Traffic
Converged VPN Solution with Integrated Threat-Protection

Firewall Performance Evaluation

- Basic Firewall
  - IP Throughput
    - Raw capability of the firewall to pass traffic from interface to interface
  - Latency
    - Time traffic delay in the firewall
    - Should be measured and reported when the firewall is at its operating load
- Traditional Enterprise Firewall
  - Connection Establishment Rate
    - Speed at which firewalls can set up connections
  - Concurrent Connection Capability
    - Total number of open connections through the firewall at any given moment
  - Connection Teardown Rate
    - Speed at which firewalls can teardown connections and free resources
- Next Generation Firewall
  - Application Transaction Rate
    - Capability of the firewall to secure discrete application-layer transactions contained in an open connection
    - May include application-layer gateways, intrusion prevention, or deep-inspection technology
    - Application transaction rate are highly data dependent

Cisco's Access Control Lists (ACL)

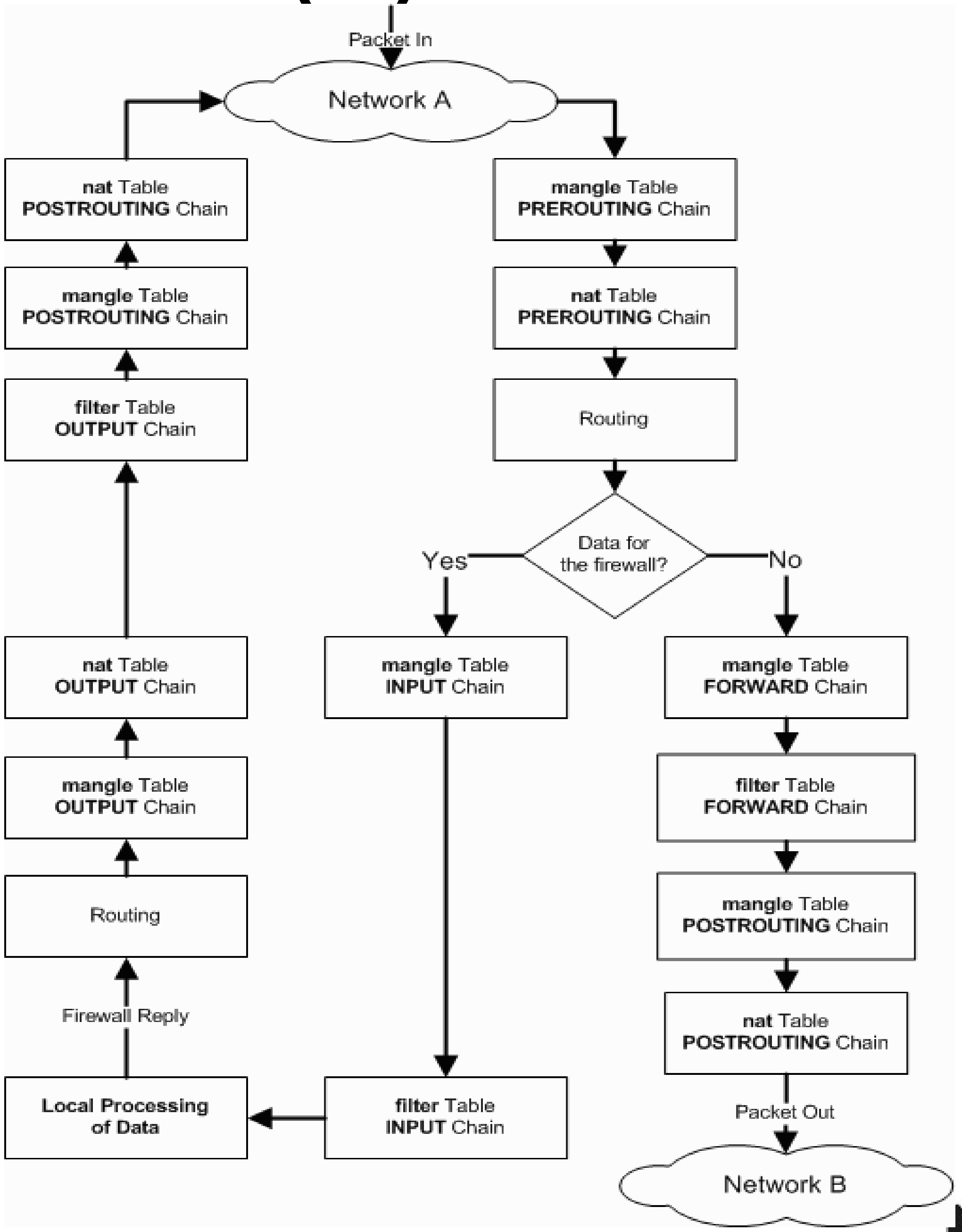
- An access list is a sequential collection of **permit** and **deny** conditions.
- Software tests packets against the conditions in an access list one by one.
- The first match determines whether the software accepts or rejects the packet.
  - Because the software stops testing conditions after the first match, the order of the conditions is critical.
- If no conditions match, the software rejects the packet.
- Can be applied to inbound or outbound traffic.

ACL Types

- Standard
  - Control traffic by the analysis of the source address of the IP packets.
  - Numbered from 1 to 99
    - Example: access-list 1 permit 10.1.1.0 0.0.0.255
- Extended
  - Control traffic by the analysis of the source and destination addresses and protocol of the IP packets.
  - Numbered from 100 to 199
    - Example: access-list 101 permit ip any 10.1.1.0 0.0.0.255
- Named
  - Allow standard and extended ACLs to be given names instead of numbers Intuitively identify an ACL using an alphanumeric name.
  - Eliminate the number limits that exist on standard and extended ACLs.
  - Named ACLs provide the ability to modify ACLs without deleting and then reconfiguring them.
    - Example: ip access-list {extended | standard} name
- Reflexive
  - Allow IP packets to be filtered based on upper-layer session information.
  - Communication in one direction opens doors in the opposite direction.
  - Generally used to allow outbound traffic and to limit inbound traffic in response to sessions that originate inside the network.
- Context-Based Access Control (CBAC)
  - Inspects traffic to discover and manage state information for TCP and UDP sessions
  - This state information is used to create temporary openings in the firewall access lists

Linux IPTables (1)

- Name of the user space tool by which administrators create rules for the packet filtering and NAT modules.
- Used to set up, maintain, and inspect the tables of IP packet filtering rules within the Linux kernel.
- Has 5 default chains:
  - INPUT, OUTPUT, FORWARD
  - PREROUTING
  - POSTROUTING
- Has 3 default tables,
  - Filter, nat and mangle
- Basic decisions
  - ACCEPT, DROP, QUEUE and RETURN
- Extended decisions
  - LOG, MARK, REJECT, TOS, SNAT, DNAT, MASQUERADE, REDIRECT, etc...
- Multiple state machines
  - Conntrack (connection tracker).


Packet In
Network A
nat Table POSTROUTING Chain
mangle Table PREROUTING Chain
mangle Table POSTROUTING Chain
nat Table PREROUTING Chain
filter Table OUTPUT Chain
Routing
Data for the firewall?
Yes
No
nat Table OUTPUT Chain
mangle Table INPUT Chain
mangle Table FORWARD Chain
mangle Table OUTPUT Chain
filter Table FORWARD Chain
Routing
mangle Table POSTROUTING Chain
Firewall Reply
nat Table POSTROUTING Chain
Local Processing of Data
filter Table INPUT Chain
Packet Out
Network B

universidade de aveiro

Linux IPTables (2)

- In addition to the built-in chains, the user can create any number of user-defined chains within each table, which allows them to group rules logically.
- Each chain contains a list of rules,
  - When a packet is sent to a chain, it is compared against each rule in the chain in order.
- The rule specifies what properties the packet must have for the rule to match (such as the port number or IP address).
- If the rule does not match, then processing continues with the next rule.
- If, however, the rule does match the packet, then the rule's target instructions are followed (and further processing of the chain is usually aborted).
- Some packet properties can only be examined in certain chains,
  - For example, the outgoing network interface is not valid in the INPUT chain.
- Some targets can only be used in certain chains, and/or certain tables,
  - For example, the SNAT target can only be used in the POSTROUTING chain of the NAT table.
- The target of a rule can be the name of a user-defined chain or one of the built-in targets (ACCEPT, DROP, RETURN, DNAT, SNAT and MASQUERADE).
- You can think of a target in the same way as a subroutine.