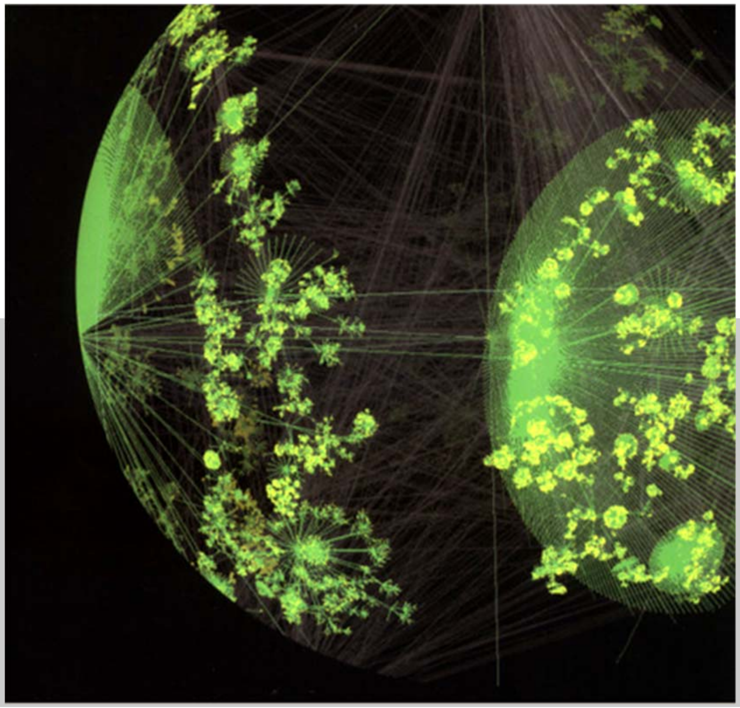


Chapter 9
Network Management & Security

TCP/IP Essentials

A Lab-Based Approach

Spring 2017

Network Management

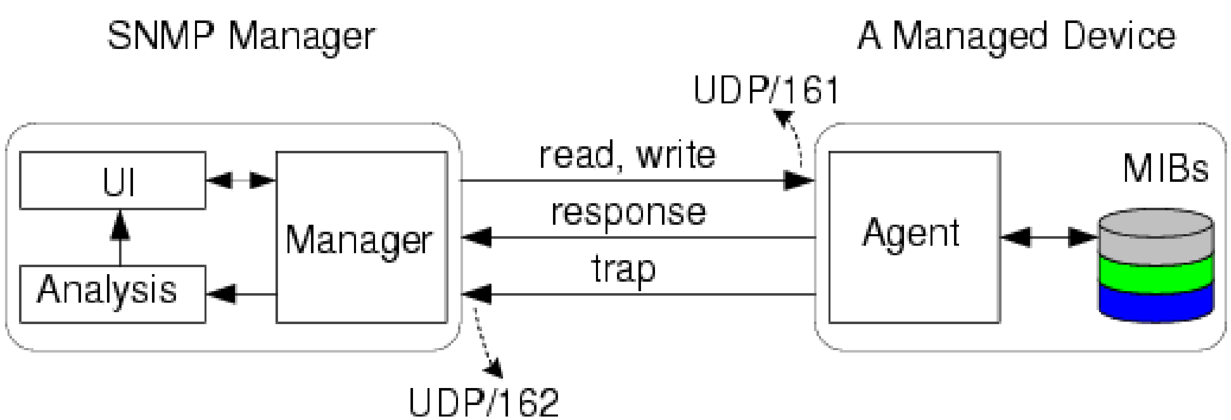
Network administrators need to

- Collect statistics from a device to see if it works properly (element management)
- Monitor network traffic load on routers to see if the load is appropriately distributed (traffic monitoring)
- Go through collected information to identify the cause when a network failure occurs (trouble shooting)

Simple Network Management Protocol (SNMP)

Simple Network Management Protocol (SNMP) is an application layer protocol for exchange management information between network devices

- Each Managed Device, a host or a router, maintains a number of Management Information Bases (MIBs)
- Each managed device has an SNMP Agent to provide interface between MIBs and an SNMP Manager
- An SNMP manager, usually implemented in Network Management System, can work with multiple SNMP agents
- Well-known UDP port number 161/162 at SNMP agent/manager



SNMP Messages

SNMP messages exchange information between an SNMP manager and an SNMP agent

- Get: fetches the value of one or more objects
- GetNext: fetches the value of the next object after the specified object
- Set: sets the value of one or more objects
- Response: returns the value of one or more objects
- Trap: reports the occurrence of some significant events in a managed device.
- Inform: reports the occurrence of some significant events in a managed device and requests a response from the manager.
- GetBulk: allows exchanging of responses with a large amount of management information.

SNMP Message Formats

Version	Community	PDU

SNMPv2 Get, GetNext, Inform, Response, Set, and Trap messages

PDU Type	Request ID	Error Status	Error Index	Object 1, Value 1	Object 2, Value 2	… …

SNMPv2 GetBulk message

PDU Type	Request ID	Non Repeaters	Max. Repetitions	Object 1, Value 1	Object 2, Value 2	… …

- Version Number
  - The version of SNMP: SNMPv1,SNMPv2, SNMPv3
  - SNMPv2 extends SNMPv1 by defining additional operations (GetBulk, Inform)
  - SNMPv3 extends SNMPv2 by adding security and remote configuration capabilities
- Community Name
  - Defines the access scope for SNMP managers and agents
  - An SNMP message carrying a different community name is discarded
- Protocol Data Unit (PDU) Type
  - Specifies the SNMP message type

SNMP Message Format (cont'd)

Version	Community	PDU

SNMPv2 Get, GetNext, Inform, Response, Set, and Trap messages

PDU Type	Request ID	Error Status	Error Index	Object 1, Value 1	Object 2, Value 2	… …

SNMPv2 GetBulk message

PDU Type	Request ID	Non Repeaters	Max. Repetitions	Object 1, Value 1	Object 2, Value 2	… …

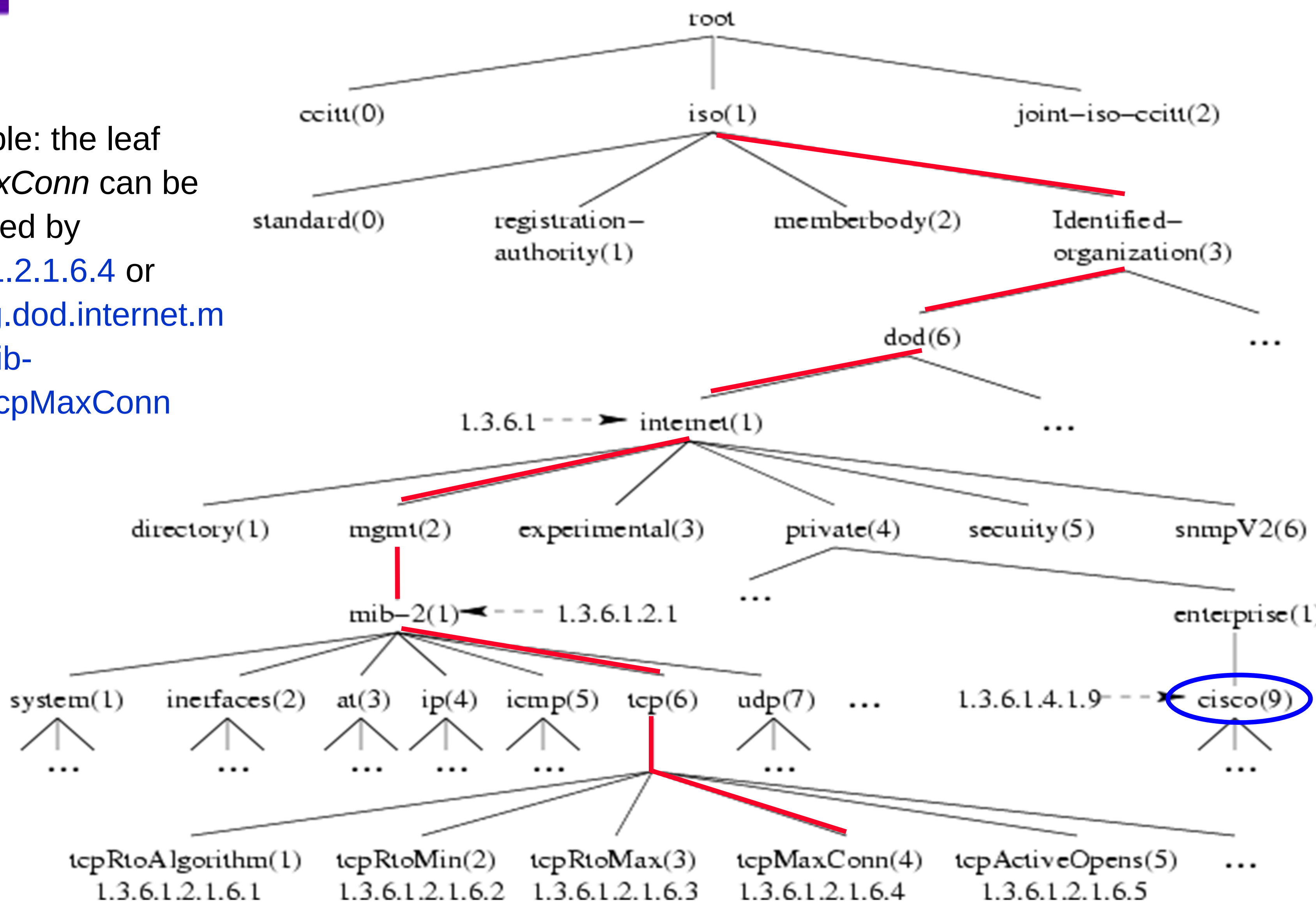
- Request ID
  - Used to match an SNMP request with the corresponding response
- Error Status
  - An integer specifying an error only set by an SNMP response
- Error Index
  - An integer offset specifying which object was in error only set by an SNMP response
- Objects and Values
  - A list of objects and their values

MIB Structure

- A managed device maintains a large number of SNMP objects to store management information
- The Structure of Management Information (SMI)
  - Defines the rules for describing management information and the data types used in SNMP
  - Data types: Integer, Octet String, Sequence
- MIB objects are organized as a tree
  - Each level of the tree consists of groups
  - Each group has its name and the associated numerical identifier
  - Leaves in the mib-2 subtree are MIB objects
  - Vendor-specific MIBs are located in the enterprise subtree
  - Each node (leaf) is identified by a concatenation of the names (or IDs) of all its predecessors starting from the root

MIB Tree Hierarchy

Example: the leaf *tcpMaxConn* can be identified by 1.3.6.1.2.1.6.4 or iso.org.dod.internet.mgmt.mib-2.tcp.tcpMaxConn



NET-SNMP

- Formerly known as UCD-SNMP
- A very popular public domain SNMP implementation
- Consists of
  - an extensible SNMP agent
  - a set of tools to request or set information from SNMP agents
  - a set of tools to generate and handle SNMP traps
  - an SNMP API library for writing SNMP related programs
- See Section 9.2.3 for details

Why Network Security?

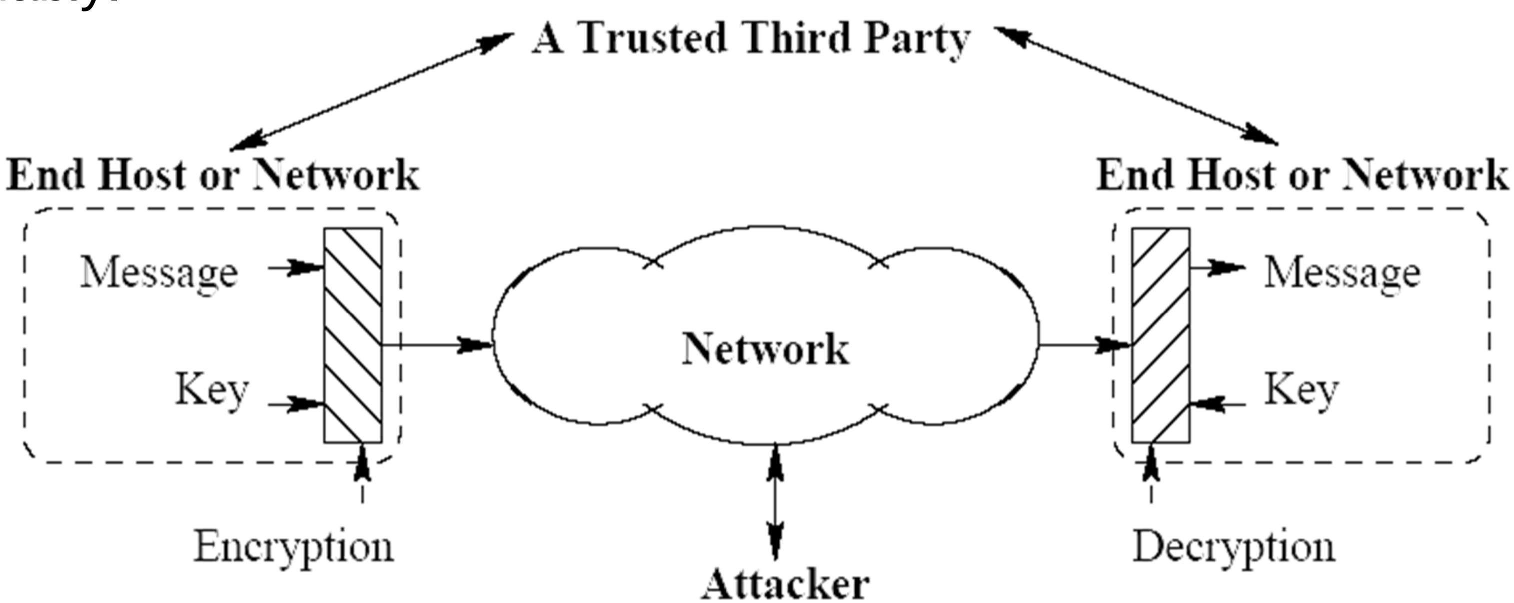
- A computer connected to Internet is exposed to attackers from all over the world
- Messages exchange between two end hosts may be intercepted or modified by an attacker
  - Many local networks are broadcast networks
  - Internet routers are shared by many data flows
- There is no global control over all the networks and users in the Internet
- An attacker may claim a false identify to gain unauthorized access to information or disrupt the normal operation of a network system

Security Elements and Services

- AAA elements of information security
  - **Authentication** to ensure users' identity – you are who you say you are
  - **Authorization** to assign legitimate privilege to users – access control
  - **Accounting** to log user behavior and resource usage for management, planning, billing, security analysis, …
- Important security services
  - **Confidentiality** protects transmitted data from analysis – no snooping, no wiretapping, a.k.a. to ensure data privacy
  - **Authenticity** identifies and ensures the origin of information
  - **Integrity** ensures that a piece of information is not altered
  - **Non-repudiation** ensures that the sender (receiver) cannot deny sending (or receiving) a piece of information
  - **Availability** ensures user accessibility to use a system
- **Network security dimensions**
  - **Communication security**
  - **Access control**

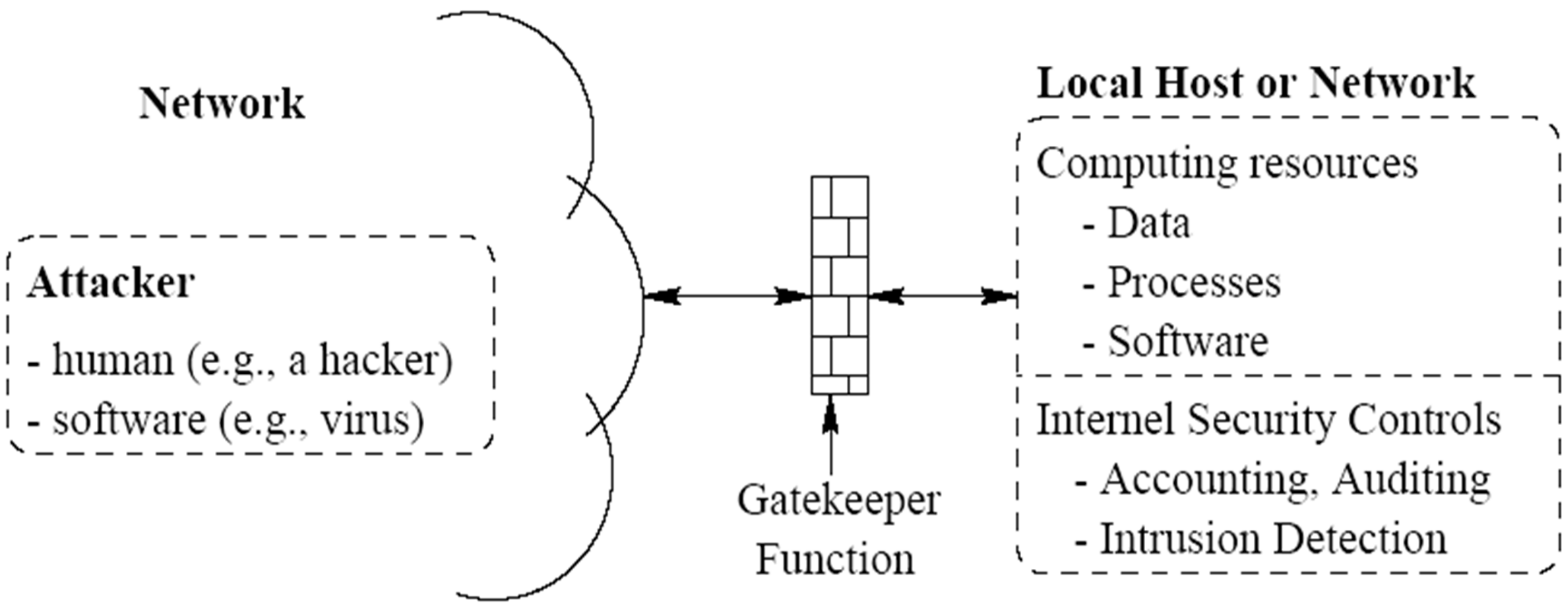
Network Security Model

- The sender encrypts the messages using a **key** before sending them out to the network
- The receiver uses the corresponding key to decrypt the message
- If the keys are kept safely, the messages will not be decipherable to an opponent
- A third party, trusted by both end users, can used to distribute the keys reliably.



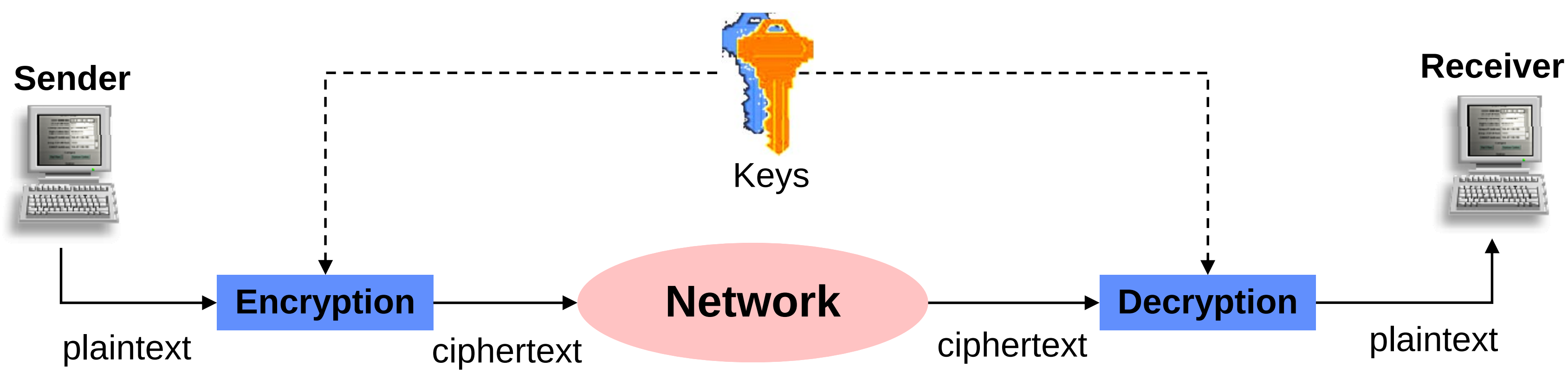
Network Access Security Model

- A gatekeeper function protects the internal information system against attack from the outside network
- The internal network performs accounting and auditing in order to detect an intrusion



Data Encryption

- Classical encryption techniques
  - Permutation: the order of the plaintext characters is changed
  - Substitution: a plaintext alphabet is mapped to a different one
- **Cipher** is the module which performs the encryption
  - **Stream ciphers** encrypt data bit by bit or byte by byte
  - **Block ciphers** first pack the data bits into a fixed length block, then encrypt the whole block into a ciphertext block.



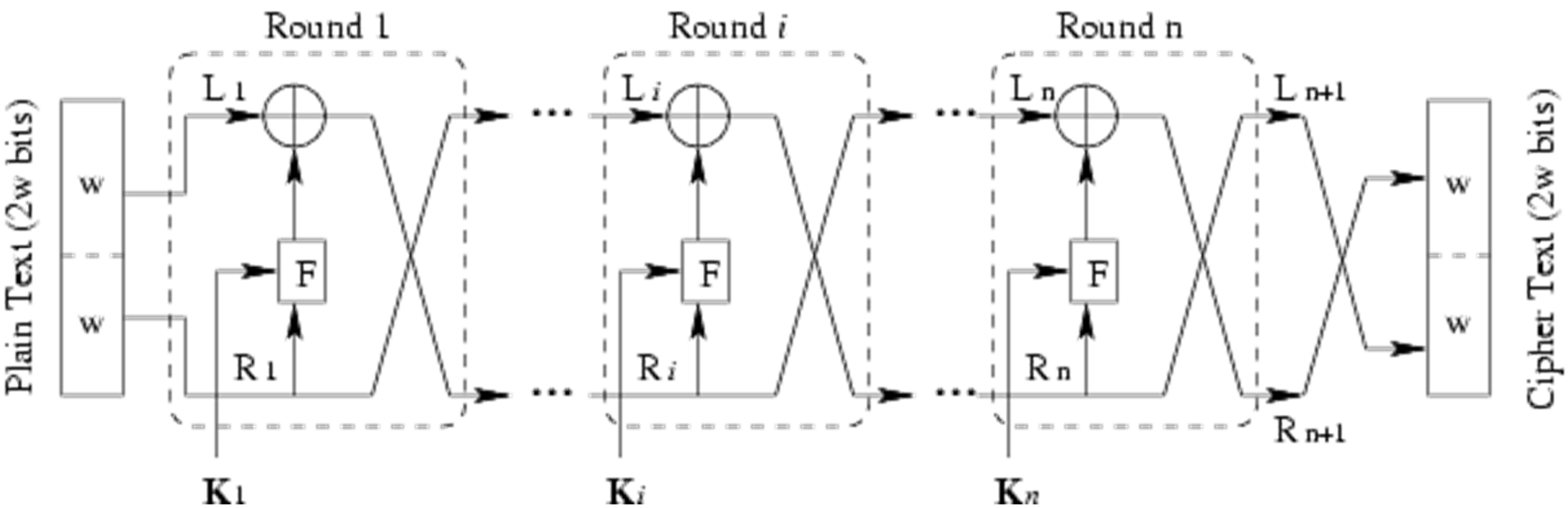
Encryption/Decryption Keys

Keys are used in encryption and decryption

- **Symmetric-key cipher**: the same key shared by both sender and receiver
- **Public-key cipher**: a private key for encryption and a public key for decryption, or vice versa
  - The public key for message encryption/decryption by a sender
  - The private key for message decryption/encryption by the receiver
- The effectiveness of the encryption schemes depends on the keys

Feistel Network Model

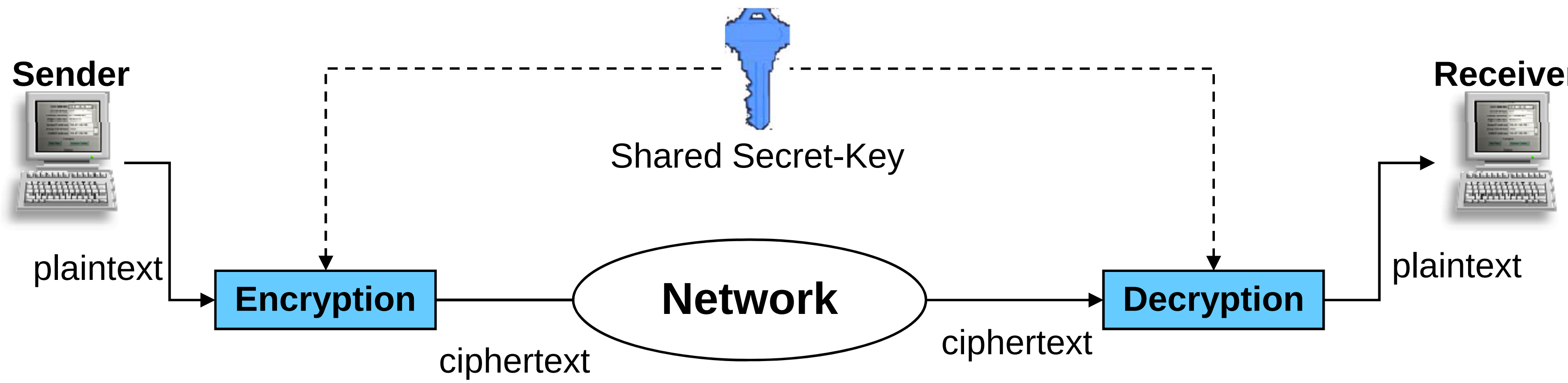
- A *2w* bit plaintext block is encrypted into a *2w* bit ciphertext block
- A number of identical blocks (called rounds) concatenate in a chain
- Operations:
  - The plaintext is first divided into two w-bit blocks, L_1 and R_1
  - R_i is first processed with a round function *F (permutation, expansion, and exclusive-OR)* using a secret key K_i
  - Compute the exclusive-OR of the L_1 and the output of *F.* The result is switched with (unprocessed) R_i and fed into the next round



Data Encryption Standard (DES)

- The most widely used encryption standard
- *Block-based cipher*, 16 rounds, 64-bit blocks, 56-bit key for 16 48-bit subkeys
- Avalanche Effect shows the strength of DES
  - –A small change in the plaintext or the 56-bit key produces a significant change in the ciphertext
  - –Makes the ciphertext difficult to decrypt by brute force
- *Symmetric cipher*, the same keys are used in the encryption and decryption
- Considered to be insecure for many applications
  - –The 56-bit key size being too small
  - –Triple DES is believed to be “secure”: use DES cipher algorithm three times to each data block
  - –**Advanced Encryption Standard (AES)** now is an encryption standard adopted by the U.S. government

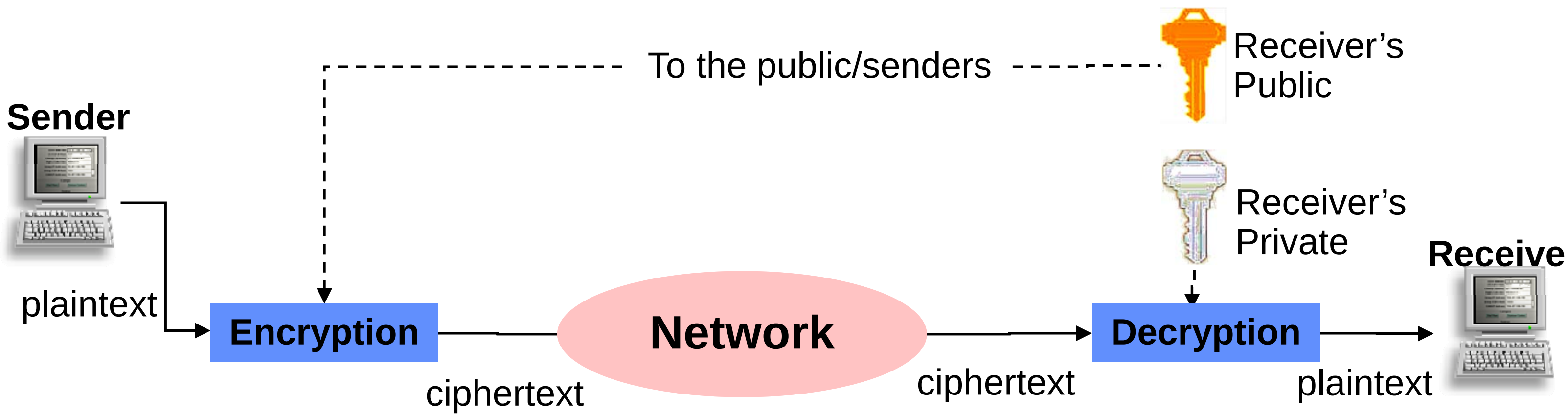
Secret-Key Encryption/Decryption



- Symmetric encryption as the same key shared by both sender and receiver
- The decryption algorithm is the inverse of the algorithm used for encryption
- Advantage
  - Efficient with relative smaller key for long messages
- Disadvantage
  - Too many keys, N(N-1)/2 keys for N users
  - Difficult to distribute shared keys (through trusted third party)

Public-Key Encryption/Decryption

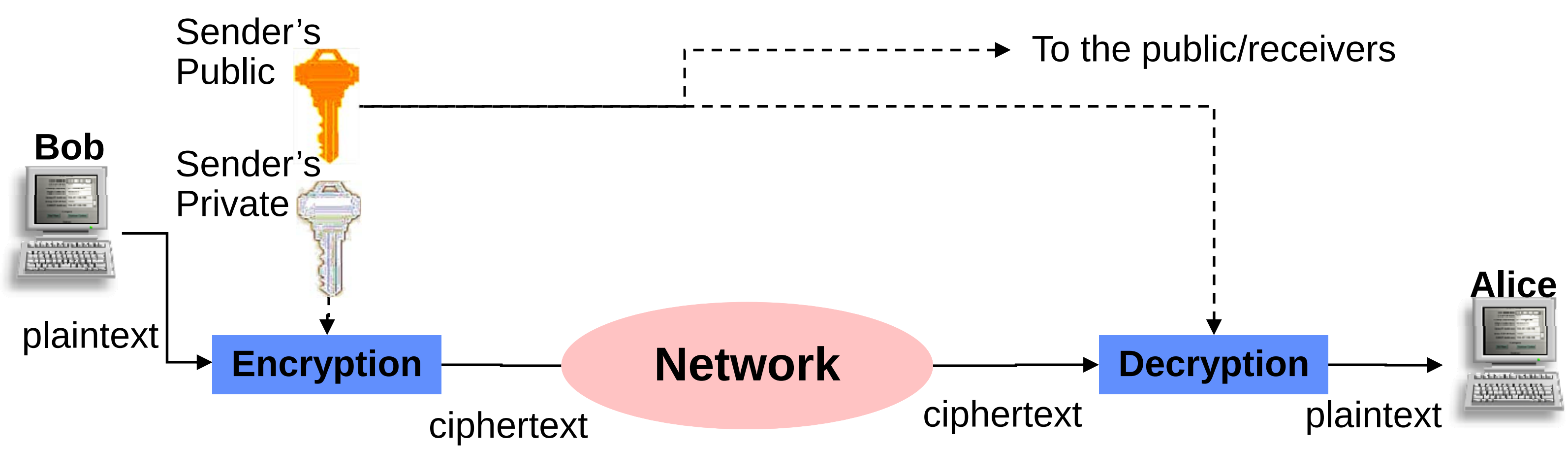
- Advantage
  - Easy to distribute public key
  - More scalable with less keys, 2N keys for N users
- Disadvantage
  - Complexity of the algorithm (okay for short messages)
  - Need receiver authentication for the public key
- A Certification Authority (CA) is used as an agency to certify the binding between a public key and the owner



Using Public-Key to provide authentication

To provide authentication

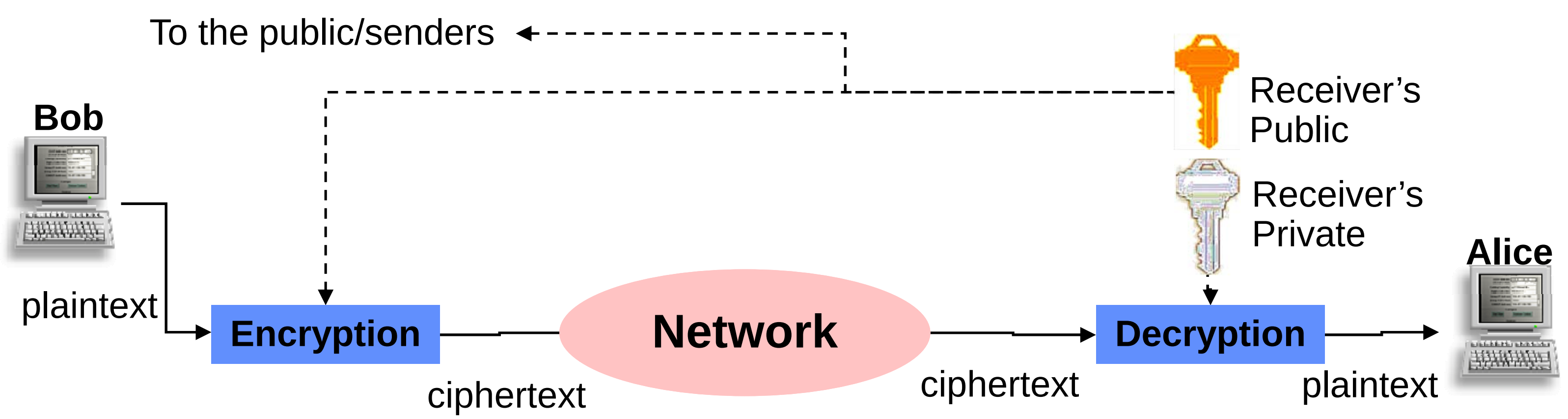
- Bob encrypts a message using his own private key and sends to Alice
- Alice decrypts the received message using Bob's public key
- Alice knows that the message can only be sent by Bob since only Bob knows his own private key
- But Bob can't use this scheme to send message only to Alice
  - All other users can decrypt the message since Bob's public key is known



Using Public-Key to provide Confidentiality

To provide confidentiality

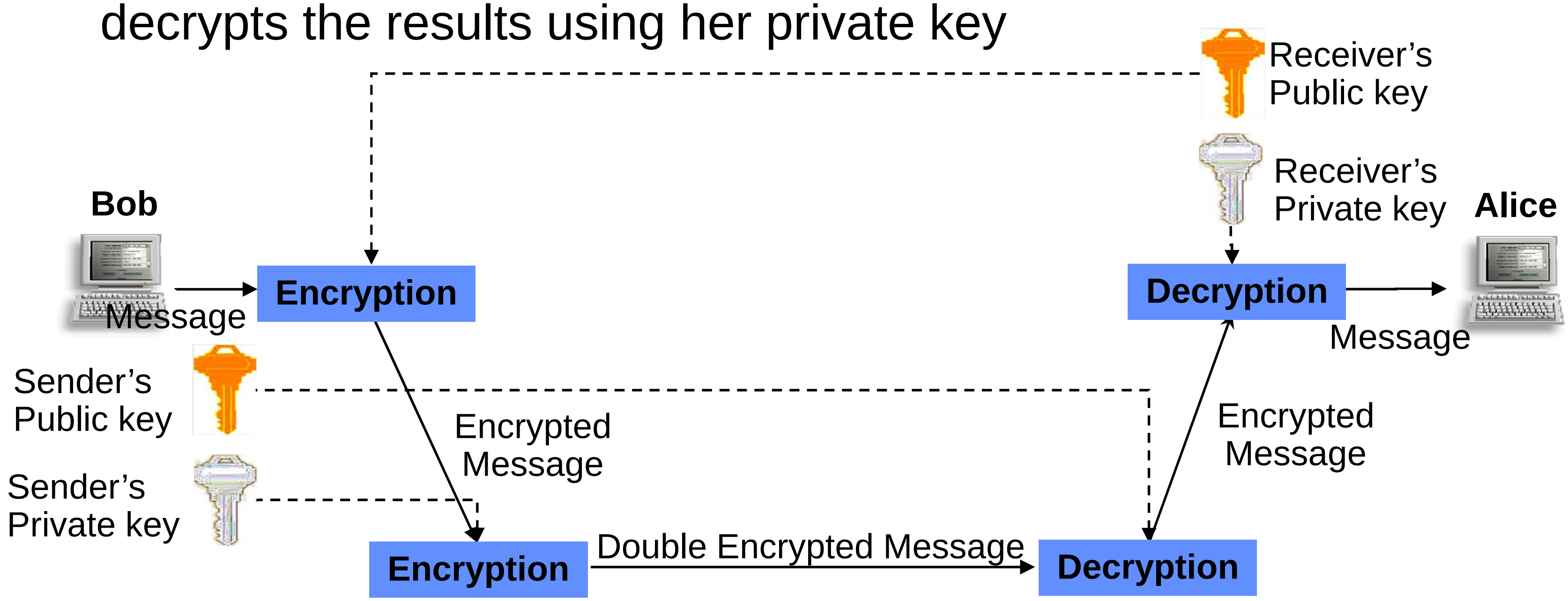
- Bob can encrypt the message using Alice's public key so that other users cannot read the message
- Alice decrypts the received message using her private key
- But Alice can't be sure the message is from Bob



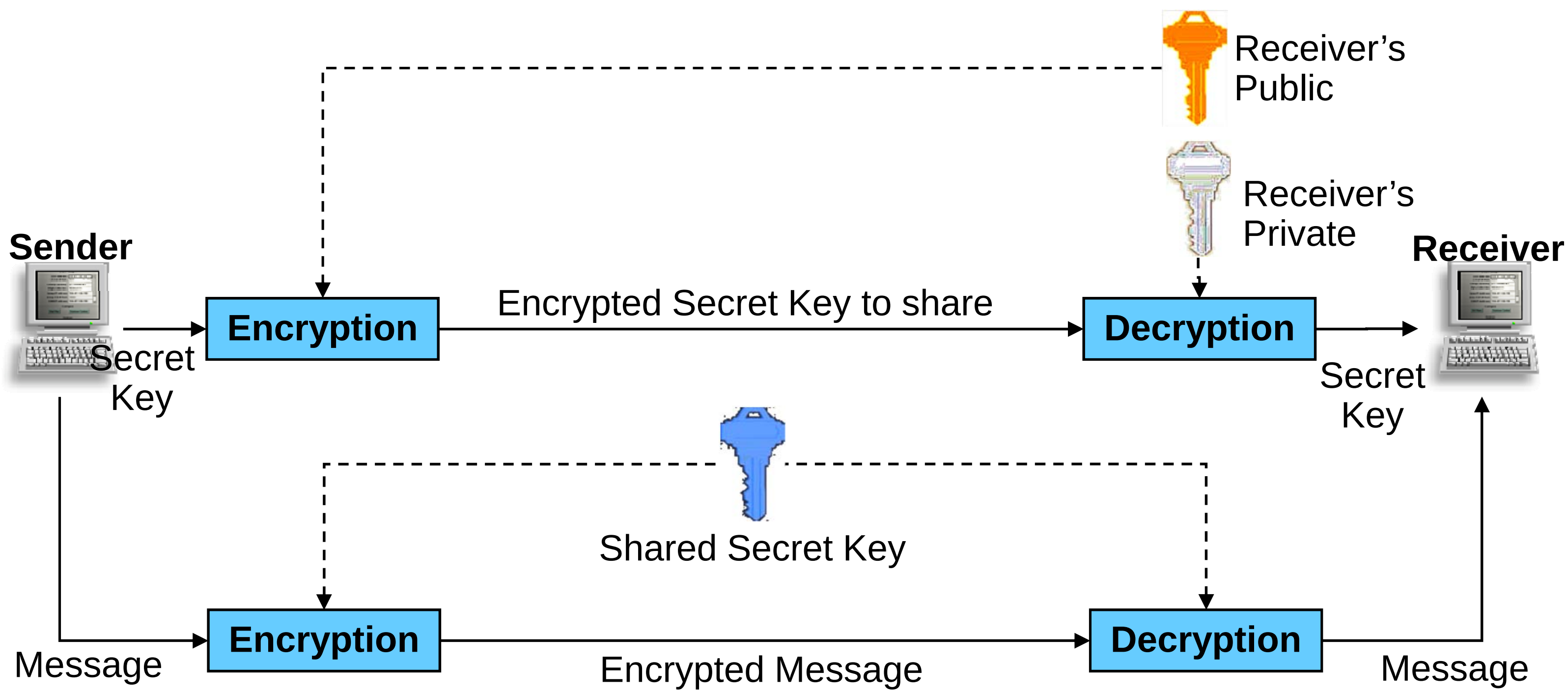
Using Public-Key (cont'd)

To provide both authentication and confidentiality

- Bob first encrypts the message using Alice's public key, then further encrypts the ciphertext with his private key
  - The 1st encryption ensures communication confidentiality
  - The 2nd encryption provides sender authentication
- Alice first decrypts the message using Bob's public key, then decrypts the results using her private key



Another Example of Using Combination of Keys



- Take the efficiency advantage from the secret-key and the advantage of easy key distribution from the public-key
- Anything else required to improve this procedure?

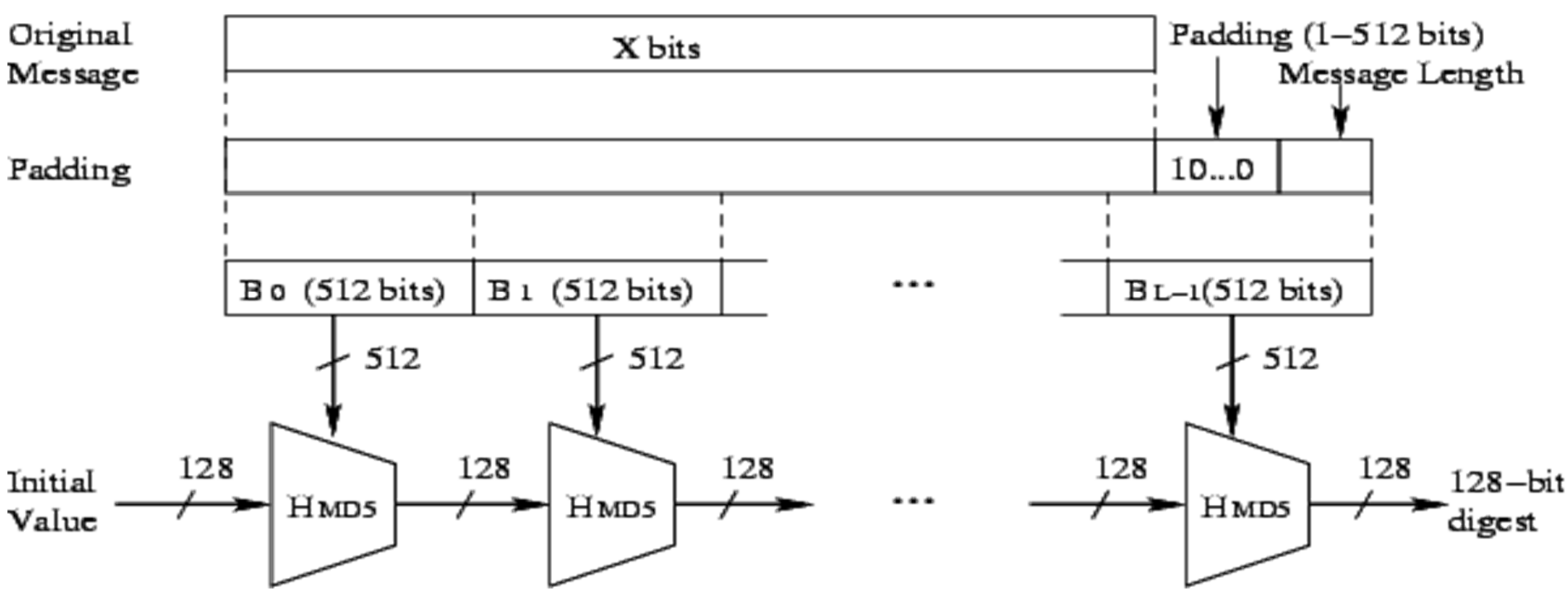
Hashing and Message Authentication

- Hashing is the operation that maps a message of variable length into a hash value with fixed length
- Hashing is not reversible
  - A hash value can be computed from a message
  - The hash value can never recover the original message
- Hashing can be used to generate a digest of the message, called the **Message Authentication Code** (MAC),
- The receiver can use the digest to verify if the message is authentic

Message Digest 5 (MD5)

Most U.S. government applications now require the SHA-2 (Secure Hash Algorithm) family with digests of 224, 256, 384, or 512 bits

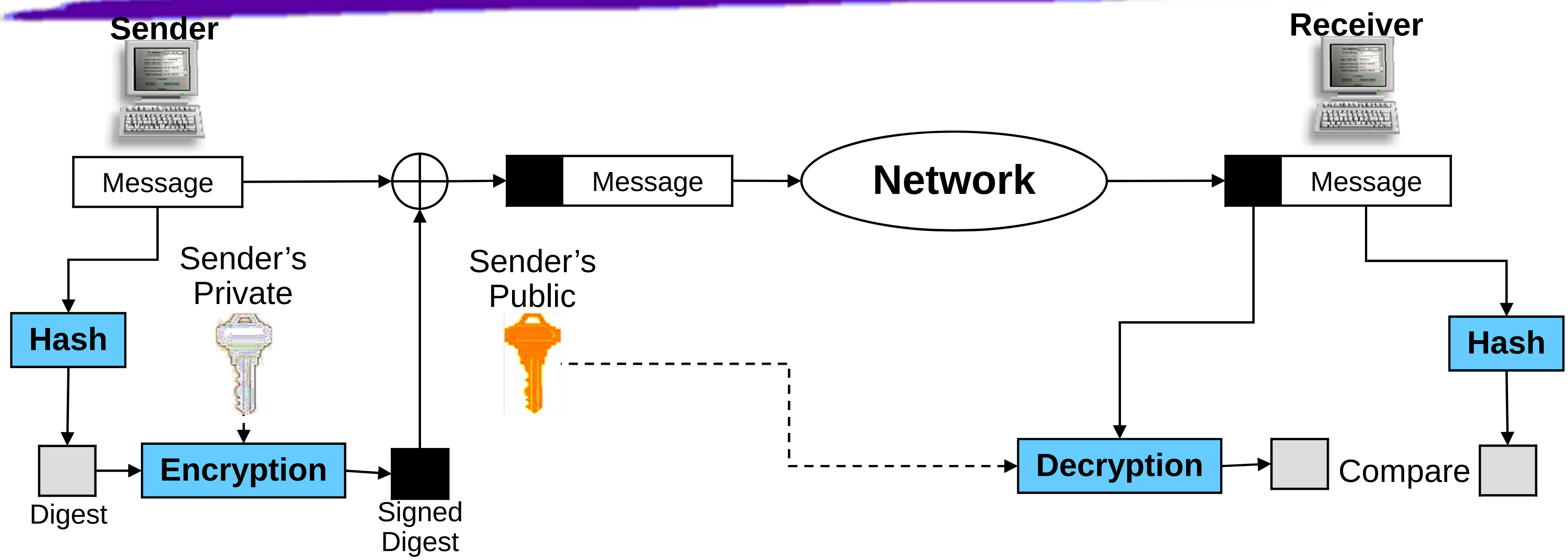
- MD5 was one of the most widely used hashing algorithms
- The sender can encrypt the MAC with the sender's private key and attach it with the original message
- The receiver may use the same MD5 algorithm for the MAC and compare it with received MAC decrypted by the sender's public key
- If the message is genuine, the two digests should be identical



Digital Signature

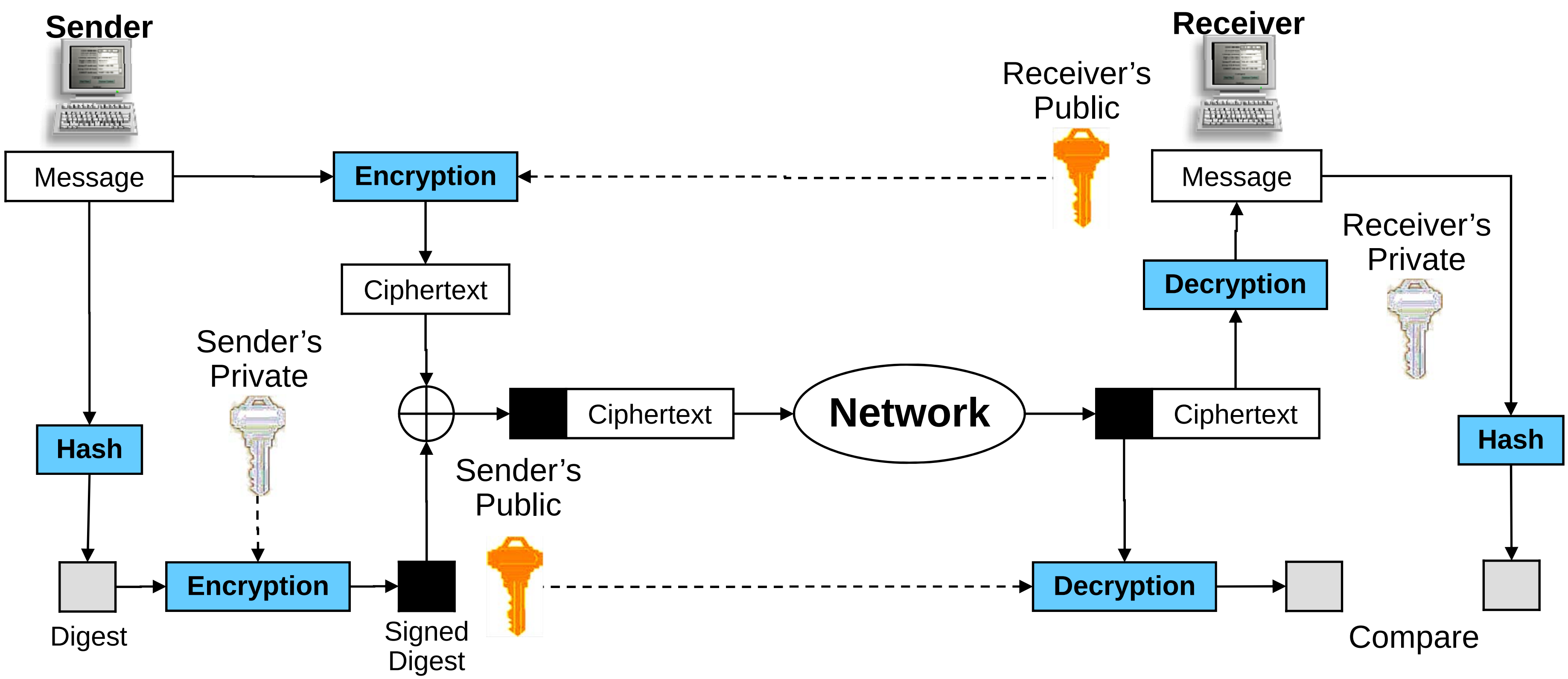
- Provide non-repudiation service when there is a lack of complete trust between the users
- Used to verify the message date/time, and to authenticate its contexts
- A digital signature is a bit pattern including
  - A digest of the message
  - The user IDs
  - A timestamp
  - Some other information
- Direct digital signature: usually encrypted using either symmetric encryption or public-key encryption
- Arbitrated digital signature: a certificate is issued by an arbitrator to the sender, may include a secret key
- Digital Signature Standard (DSS)
  - Widely used, hashing, public-key encryption

Example: Digital Signature



- Digital signature cannot be achieved using only secret keys
- How to overcome the inefficiency of public-key encryption for lengthy document with digital signature?
  - Using *Hash Function* to create a fixed-size digest from a document of any length
  - Signing the document digest and attaching it with the document
- Digital signature provides integrity, authentication, and nonrepudiation

Example: Signed Message with Confidentiality



- Provide integrity, authentication, non-repudiation, and confidentiality

Secure Shell (SSH) protocol

- **Application layer security**
- A set of protocols for secure remote login and other secure network services over an insecure network
  - Replace transitional remote access protocols
  - Support almost any kind of public-key algorithm and various types of authentication
  - SSH client and server use digital signatures to verify their identity.
  - All communication between the client and server is encrypted.
- Major components:
  - The Transport Layer Protocol (SSH-TRANS): provides server authentication
  - User Authentication Protocol (SSH-USERAUTH): authenticates the client-side user to the server
  - Connection Protocol (SSH-CONNECT): multiplexes the encrypted tunnel into several logical channels

OpenSSH

- **A public domain implementation of SSH**
- Includes ssh, sshd, scp, sftp, sftp-server, and other basic utilities
- Supports Linux and Solaris platforms
- Provides tools for key management
  - ssh-keygen: creates keys for public-key authentication
  - ssh-agent: an authentication agent holding RSA keys
  - ssh-add: used to register new keys with the SSH agent
  - ssh-keyscan: used to gather SSH public keys
- Client programs:
  - ssh, a secure client for logging into a remote machine and executing commands there
    - e.g., to login into shakti as user guest:
      ssh guest@128.238.66.100
  - scp, a secure client for copying files between hosts
    - e.g., to upload a file foo.txt to host shakti:
      scp foo.txt guest@128.238.66.100:/home/guest/foo.txt
  - sftp, a secure interactive file transfer program

Kerberos

- **A network authentication protocol**
- Developed by the MIT Project Athena team
- Uses symmetric key encryption for authenticating users for network services
- Uses a trusted Authentication Server and a Ticket-Granting Server (TGS) to provide two types of tickets to a user
  - Ticket-granting ticket
  - Service-granting tickets
  - Perform the ticket-granting ticket application once per user login
  - Perform the service-granting ticket application once per service
  - The user password is not transmitted, thus cannot sniffed by an attacker

Kerberos Operation

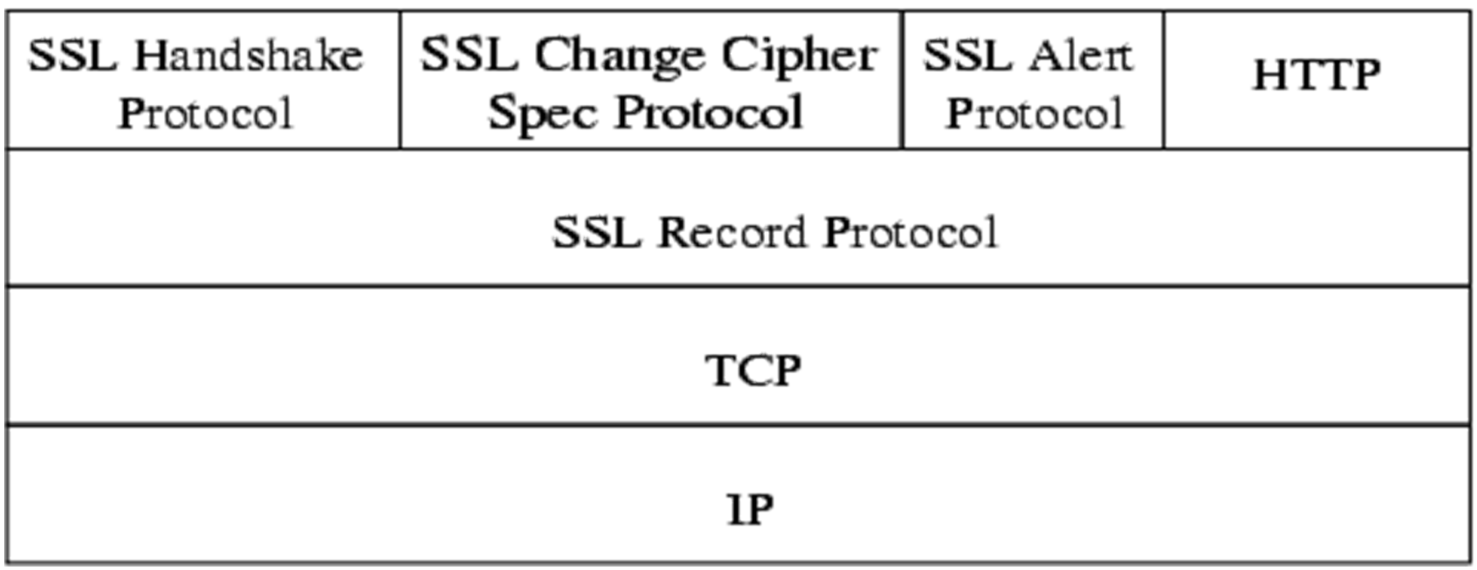
- When a user logs on to a computer
  - A request for the ticket-granting ticket is sent to the Authentication Server
  - The Authentication Server verifies the user ID and then returns a ticket-granting ticket which is encrypted using the user's key
- Decrypt the returned ticket-granting ticket by using the user's key
  - The ticket is valid for a period of time and stored for future use
  - The user's key is computed from the user's password, no need to transmit the user's password in the network
- When the user requests a network service,
  - The ticket-granting ticket is used to request the corresponding service-granting ticket
  - The TGS uses the received ticket-granting ticket to authenticate the request and returns the requested service-granting ticket to the user
- The user request the network service using the service-granting ticket

Web Security

- HTTP requests and responses are sent as plaintext
- Extra security for web service is needed in some situations
  - e.g. financial transactions
- Web security can be provided by
  - Using the application layer security protocols
  - Using the Secure Sockets Layer (SSL) in the transport layer
  - Using IP security (IPsec) in the network Layer

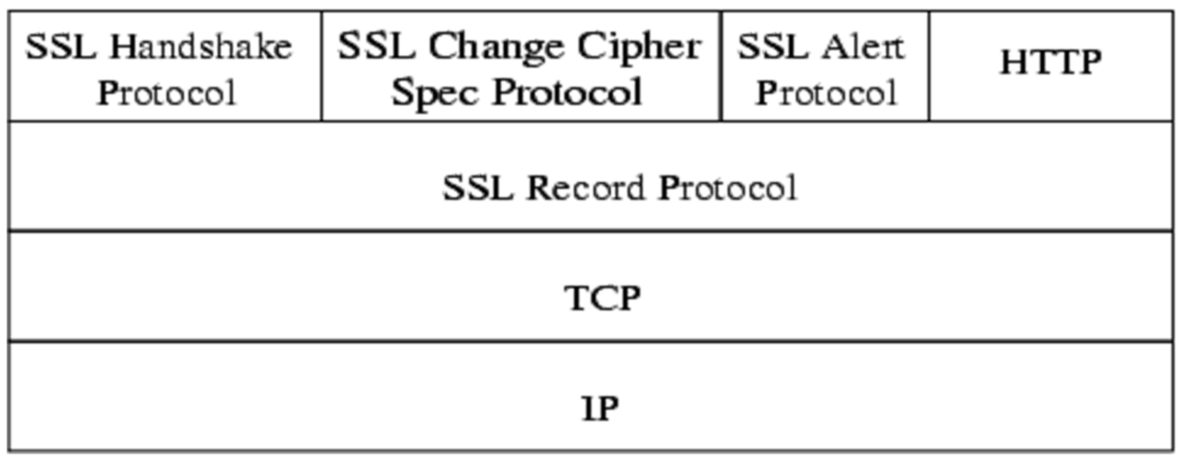
Secure Sockets Layer (SSL) protocol

- Provides secure communications between a client and a server
- Uses TCP’s reliable transport service for data communication
- Independent of the higher layer application protocols
- Application protocols (HTTP, Telnet, FTP, etc.) can use SSL for secure communication
- Consists of four protocols



SSL Protocols

- SSL can
  - negotiate an encryption algorithm and session key
  - authenticate for the secure connection
- SSL Handshake Protocol: for client and server to
  - Authenticate each other
  - Negotiate and encryption algorithm and a MAC algorithm
  - Exchange the encryption keys
- SSL Change Cipher Spec Protocol
  - Updates the set of ciphers to be used on the connection
- SSL Alert Protocol
  - Deliver SSL-related alerts to the peer entity
- SSL Record Protocol
  - all higher layer messages are encapsulated in SSL records



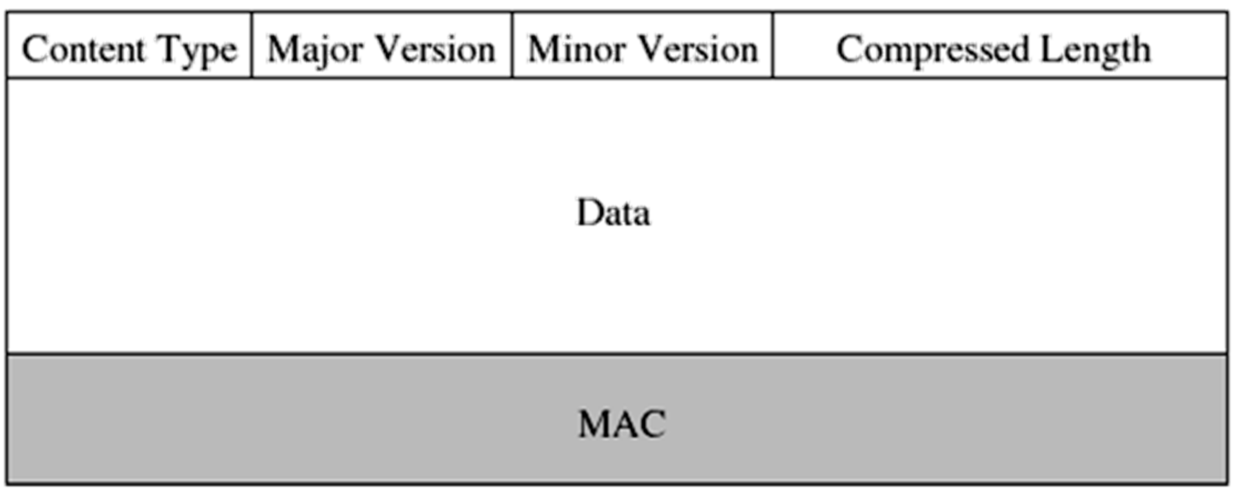
SSL Record Message Format

The SSL record header consists of

- Content Type field, 8 bits
- Major Version field, 8 bits
- Minor Version field, 8 bits
- Compressed Length field, 16 bits

The SSL record data section consists of

- Message Authentication Code (MAC)
- Actual data
- Possible padding bytes



Generating an SSL Record Message

- A higher layer message is first fragmented to fixed length blocks
- Each block may then be compressed
- The MAC is computed using a hash function
- Inputs of the hash function
  - Possibly compressed data
  - A secret key
  - A 32-bit long sequence number
- The data and the MAC are encrypted and the SSL record header is appended

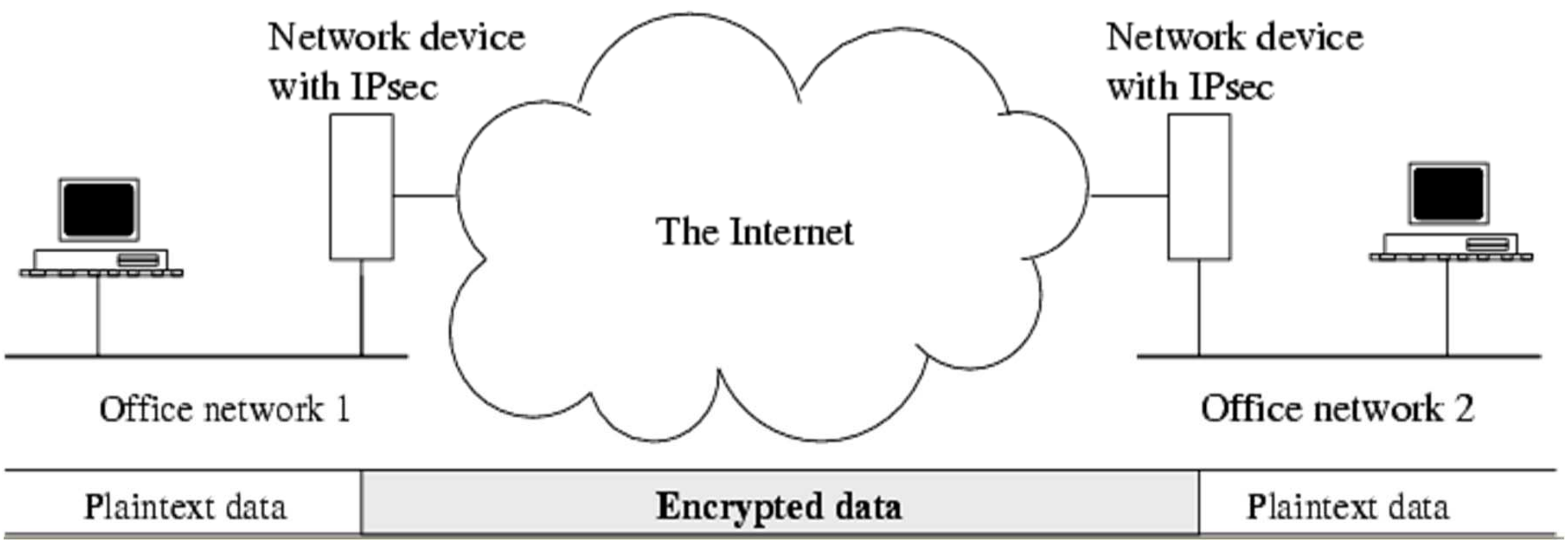
Secure Apache server

- Uses SSL to provide a secure web service
  - Certification of server and client
  - Encryption of HTTP messages
- Uses TCP port 443 with URLs starting with https://
  - Unsecured Apache servers, TCP port 80, http://
- To set up a secure Apache server:
  - mod_ssl Apache loadable module
  - openssl utility
  - Please refer to section 9.6.2 for detailed steps

Network Layer Security

IP security (IPsec)

- A typical application
  - Two offices are connected by a secure channel provided by IPsec
  - Application data is transmitted as plaintext in regular IP datagrams in each office network
  - The security-related operations are performed at the two IPsec-capable devices, transparent to the users
  - Also called Virtual Private Network (VPN)?



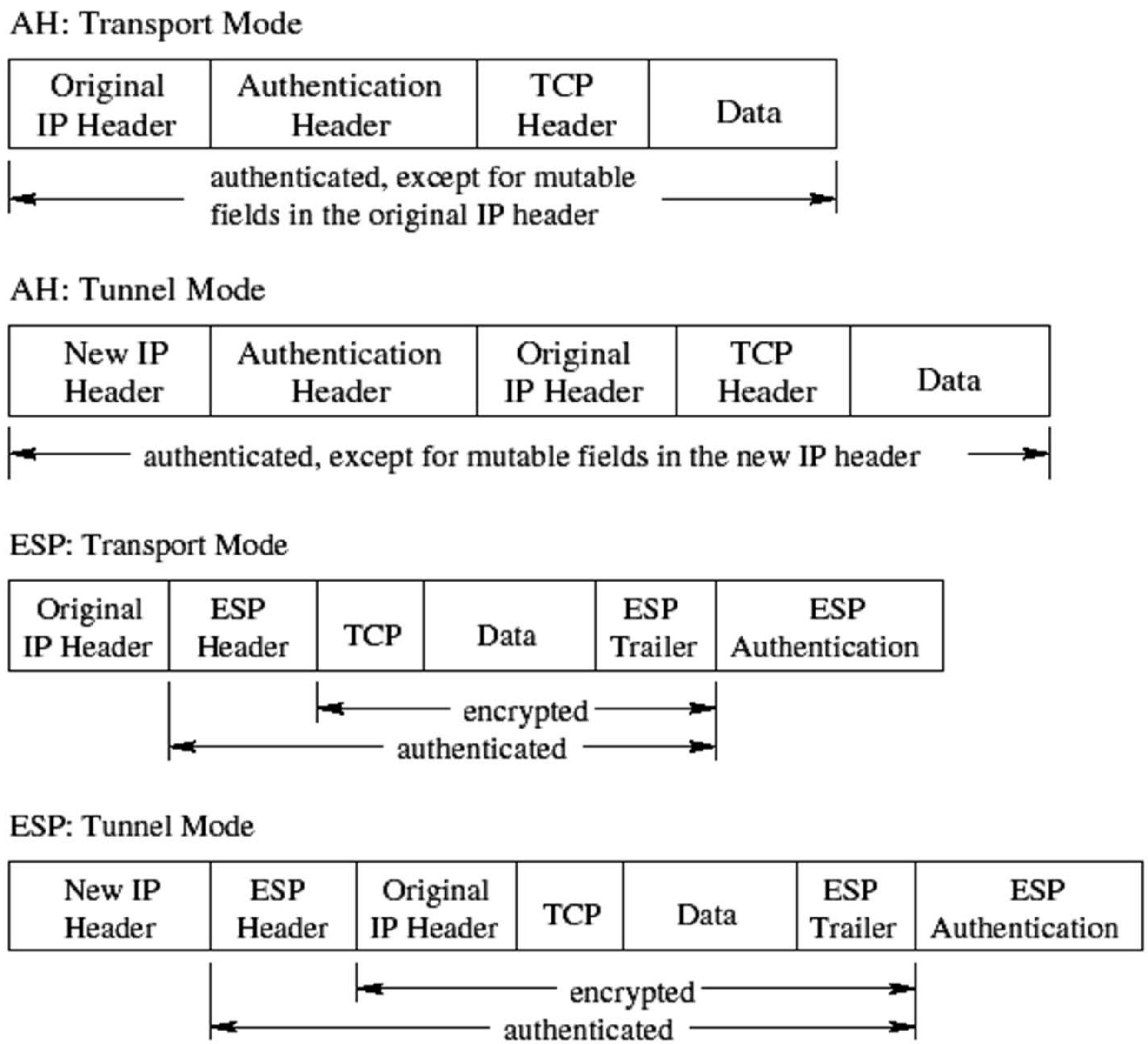
IP security (IPsec)

- A set of protocols providing authentication and confidentiality services in the network layer
- Protects all distributed applications
- Higher layer protocols can enjoy the protection provided by IPsec transparently
- Two protocols
  - Authentication protocol, using an Authentication Header (AH)
  - Encryption/authentication protocol, called the Encapsulating Security Payload (ESP)
- Two modes of operation
  - Transport mode: provides protection for upper-layer protocols
  - Tunnel mode: protects the entire IP datagram

IPsec Encapsulation

IP security (IPsec)

- Two protocols:
  - AH
  - ESP
- Two modes
  - Transport mode
  - Tunnel mode



System Security

Firewalls

- A device or program inserted between a private network and the Internet to control access
- Can be used to
  - block undesired traffic from the outside
  - prevent an internal user from receiving an unauthorized external network service
- Usually is the only access point of a private network
- Three type of firewall functions
  - Packet filter: blocks selected network packets
  - Application gateway, or a proxy server: regulates outbound traffic, acts as a relay for a specific application
  - Circuit-level gateway: acts like a switch board, switching an internal connection to another external connection

System Security (cont'd)

iptables

- The default firewall in Linux
- Firewall policy (rule)
  - Consists of
    - > A condition, e.g., destination port number of a packet
    - > The operation on the packets that satisfy the condition
  - Rules are organized into tables in Linux
    - > Filter table: default table for filtering packets
    - > Nat table: alter packets that create a new connection
    - > Mangle table: for specific types of packet alteration
- In iptables, a packet is first dispatched to the corresponding chain, then is checked against each rule in that chain. If there is a match, the target defined in the rule is performed on the packet.

System Security (cont'd)

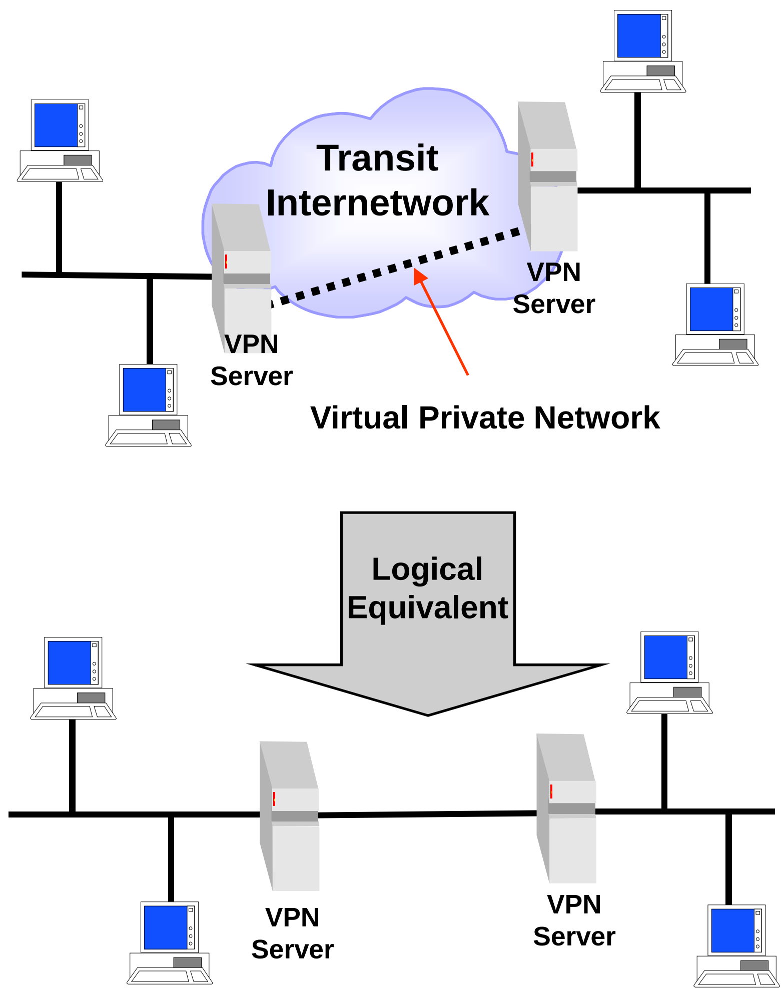
Auditing and intrusion detection

- All Unix and Linux log network events and user activity
- An intruder may be identified by examining the log files
- Commands to monitor active users or check network services (see section 9.8.3)
- Tripwire: a public domain tool, detects and reports changes in the system files

Network Layer Security Example
Virtual Private Network (VPN)

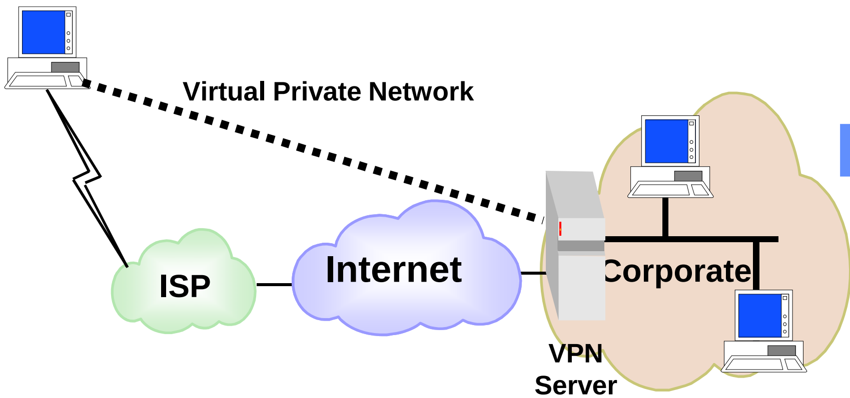
Basic Requirements

- User Authentication
- Address Management
- Data Encryption
- Key Management
- Multiprotocol Support

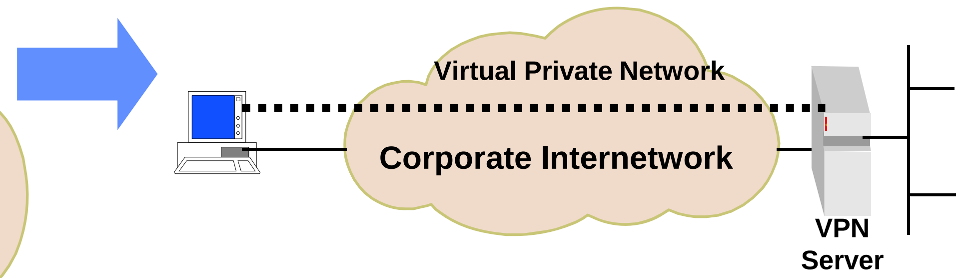


Common Uses of VPNs

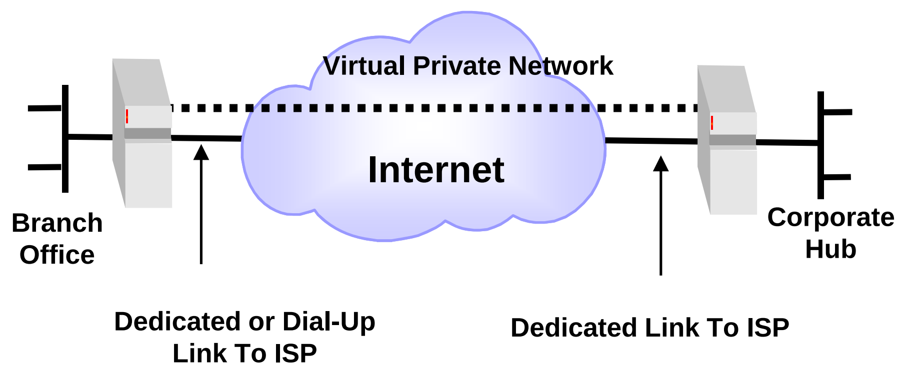
Remote User Access Over Internet



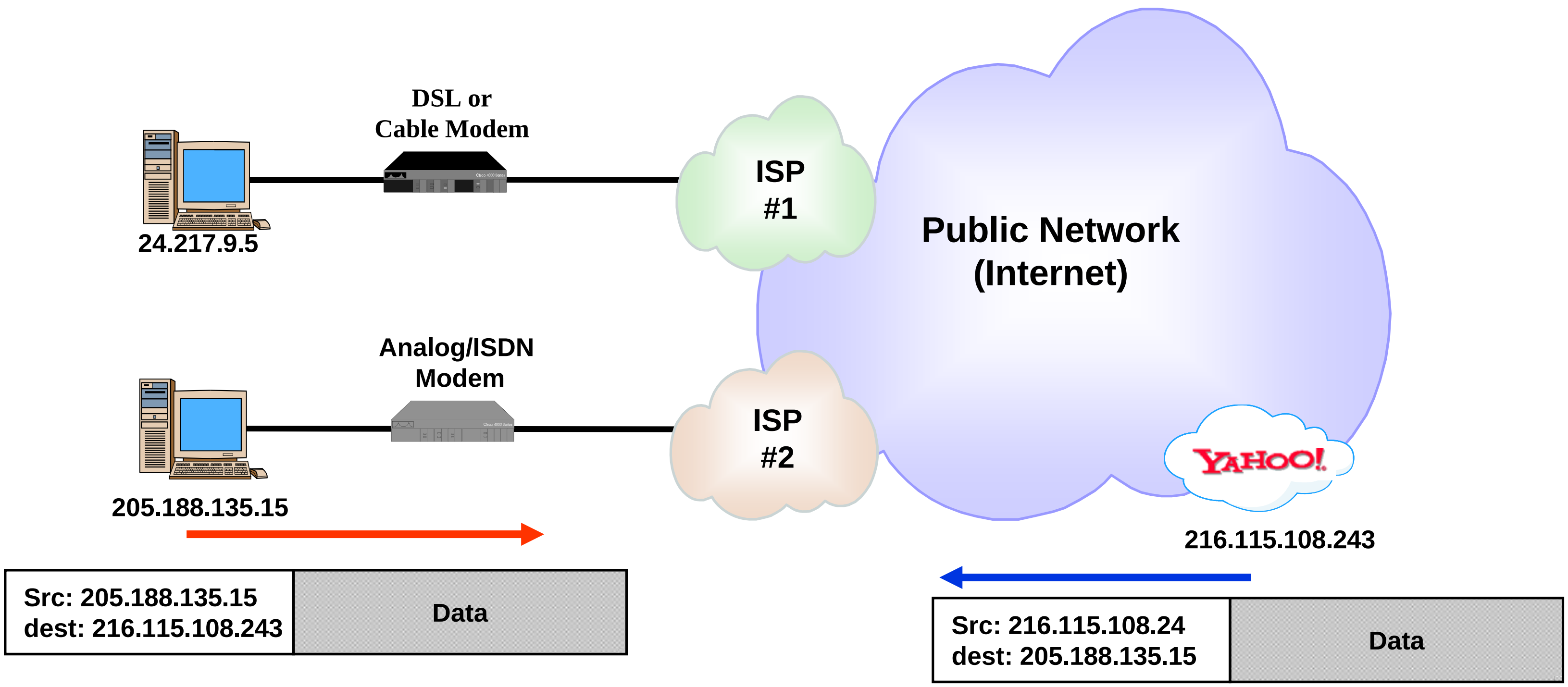
Connecting Computers Over Intranet



Connecting Networks Over Internet

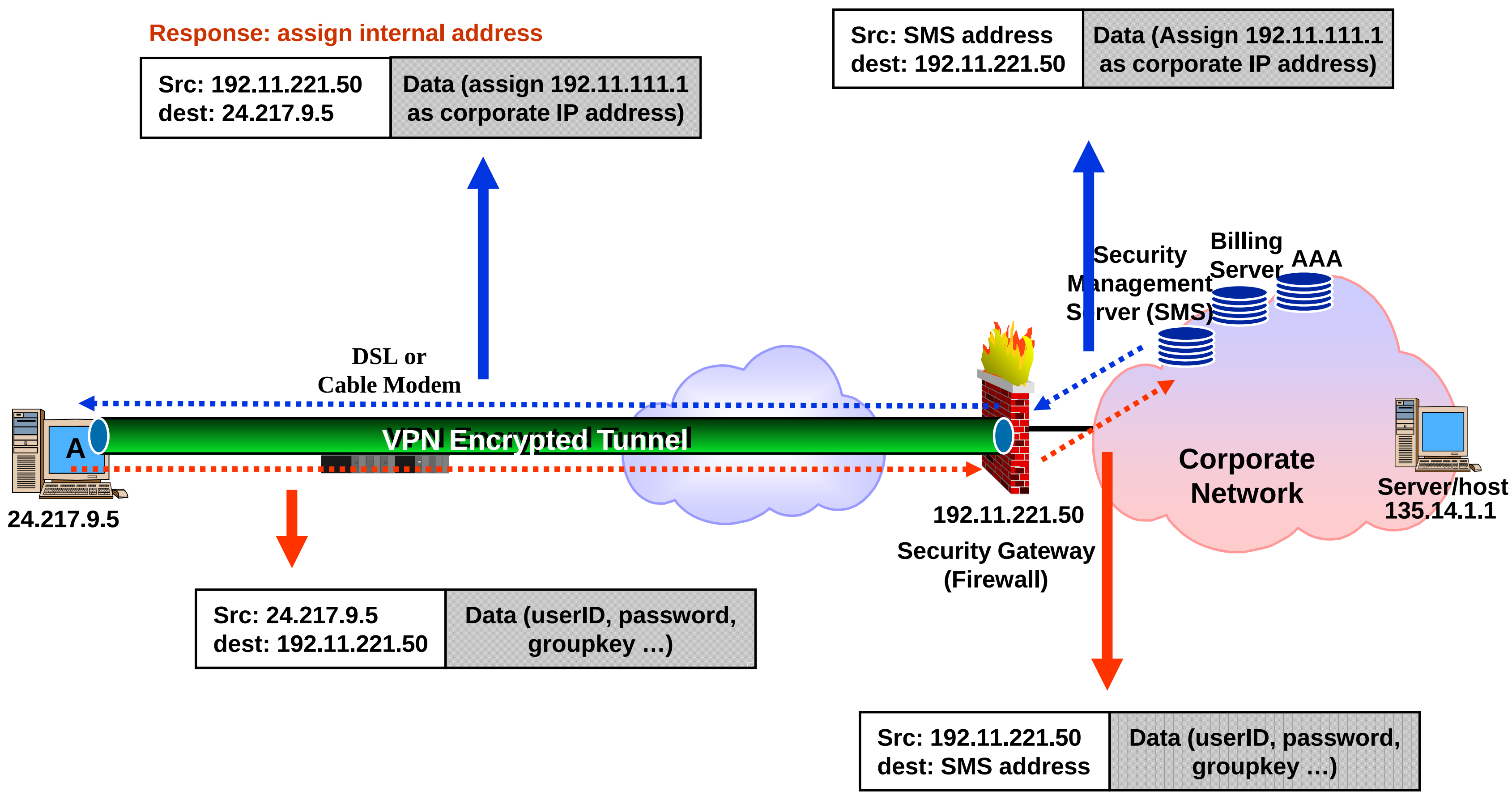


Internet Access without Tunnel

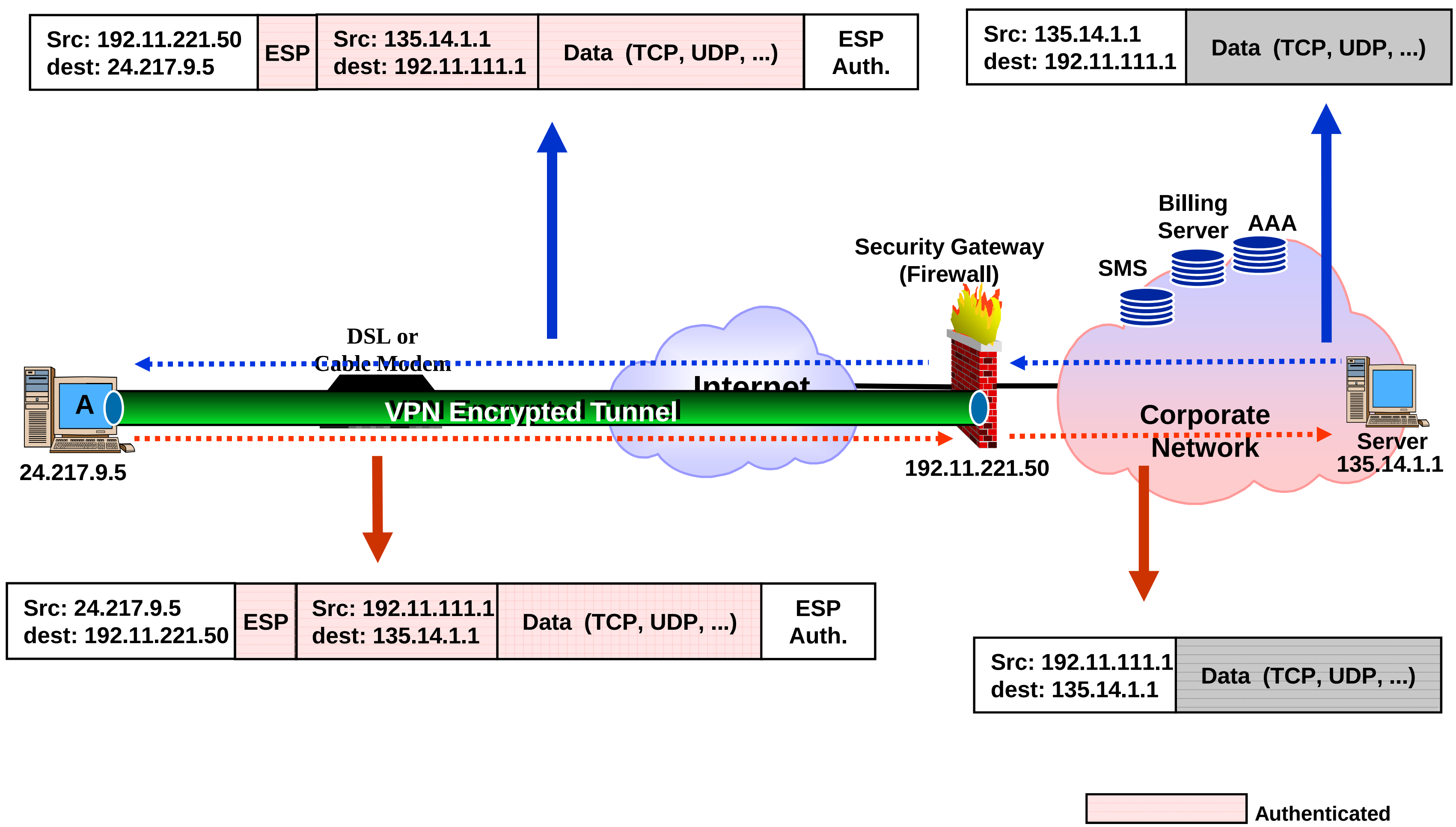


Internet Access with IPSec Tunnel

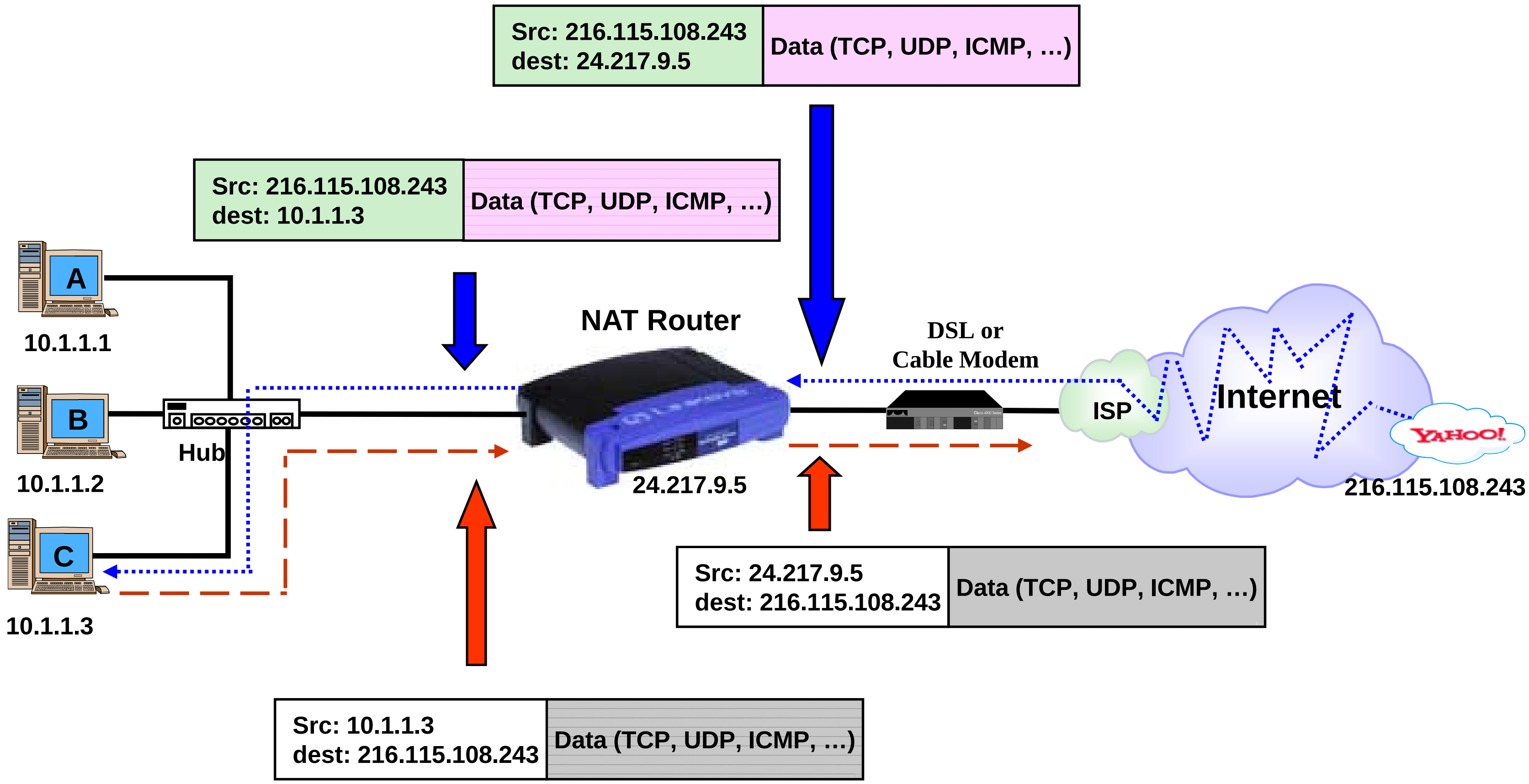
Establish VPN Tunnel



Internet Access with IPSec Tunnel
Data Transfer

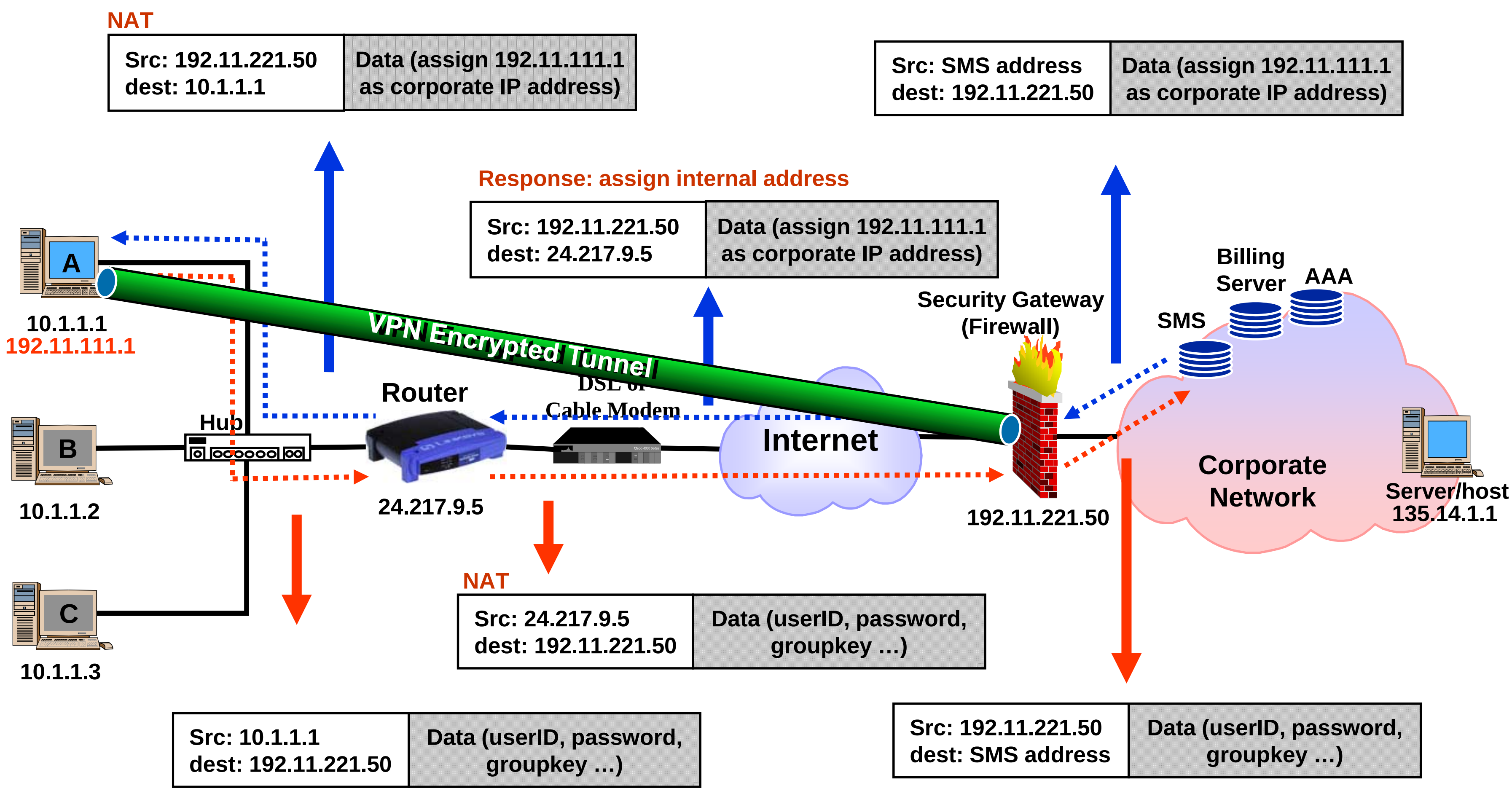


Home LAN Internet Access without IPSec Tunnel



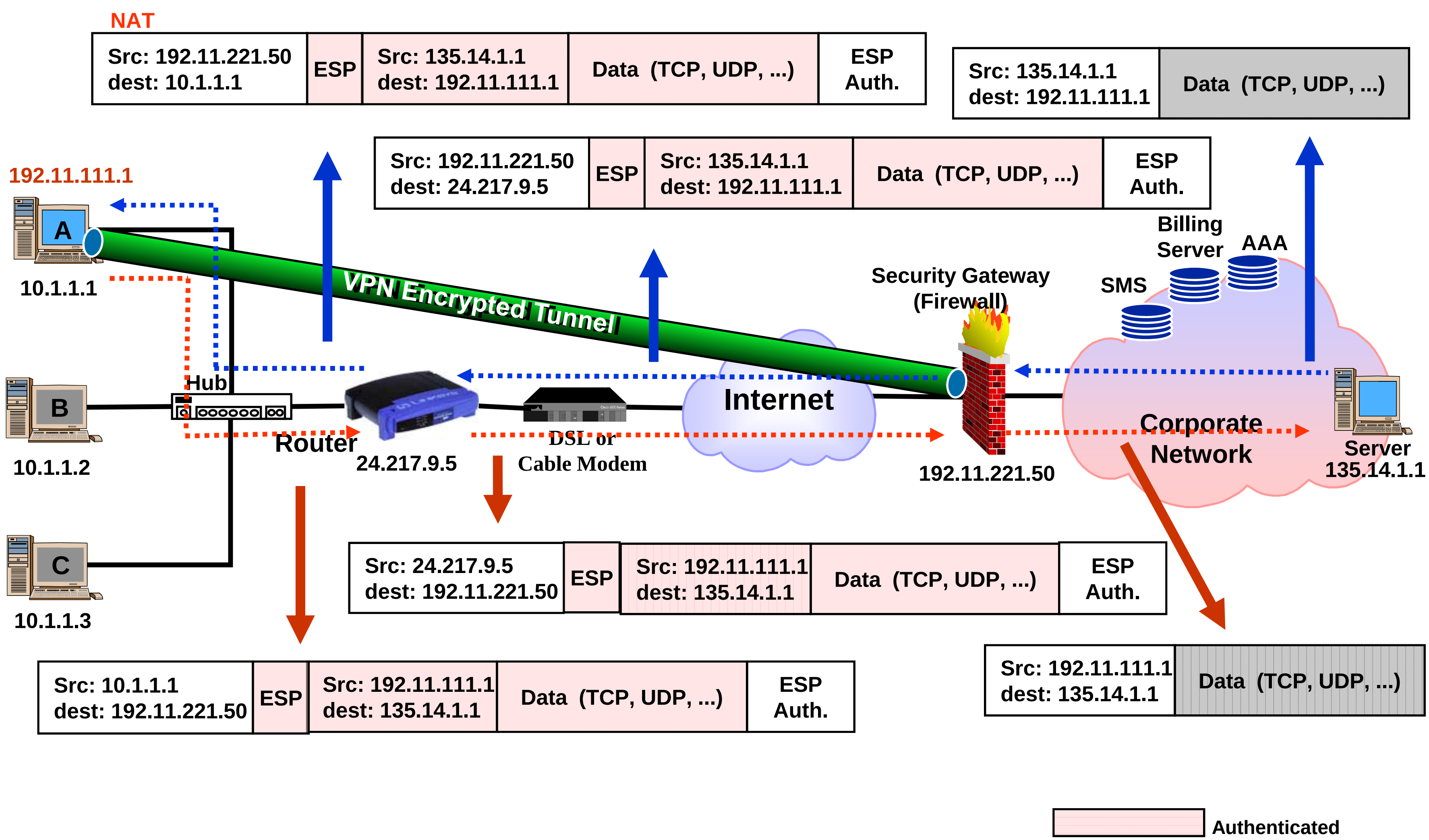
Home LAN Internet Access with IPSec Tunnel

Establish VPN Tunnel



Home LAN Internet Access with IPSec Tunnel

Data Transfer



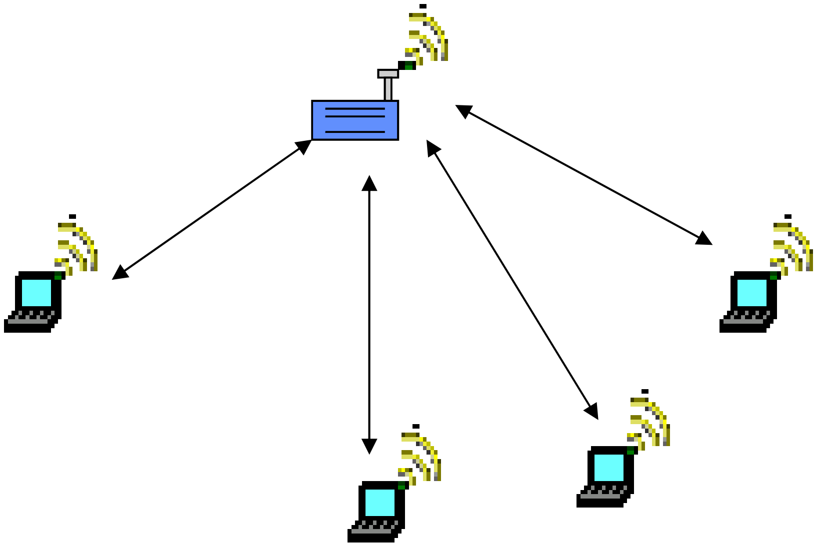
WLAN Access & Privacy Services

Wired connection, the basic characteristic of wired LAN, is not inherent in a wireless LAN

- The physical connection provides a form of authentication
- In WLAN, any wireless station (STA) within the radio range of other devices may try to receive or/and transmit data

IEEE 802.11 features to provide secured WLAN connection

- Authentication to ensure the identity of a communicated party
- De-authentication to terminate an existing authentication
- Privacy with data encryption



Discovering APs

- Media's sensational stories about "War Driving"
  - Load laptop and GPS in car and drive
  - War driving software listens and builds map of all 802.11 networks around While you drive
- But 802.11 encourages AP auto-discovery by STAs
  - A basic AP feature to avoid some manual configuration in wireless stations
  - AP discovery does not compromise WLAN security in any aspect
- War driving software relies on two basic techniques
  - Querying the WLAN interface to observe all 802.11 beacon frames
  - Monitoring the beacon frames and the associated WLAN connection

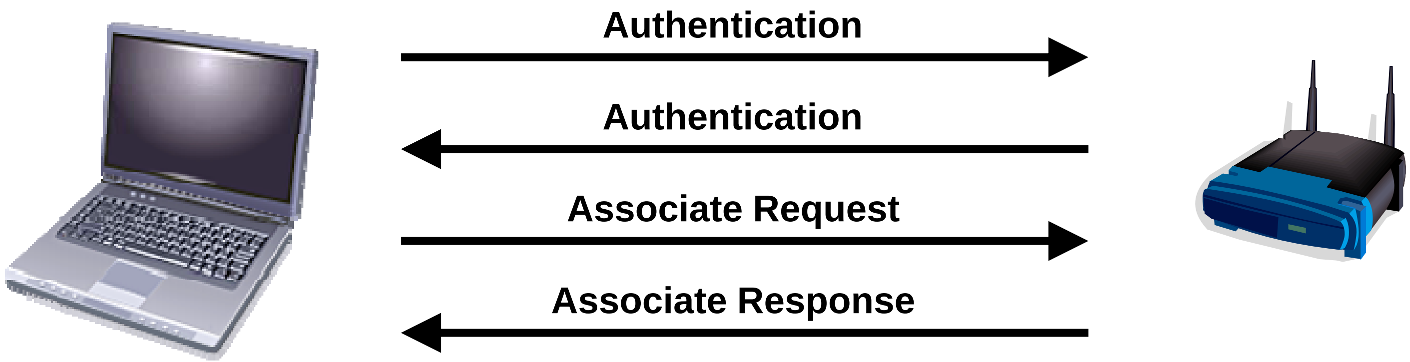
802.11 Beacons

- All wireless APs periodically send out beacon frames
  - Default rate at 10 beacons per second
  - Beacon frames are a type of management frame
  - Each type of 802.11 management frames and control frames are sent unencrypted at an average rate of 1 Mbps
- Beacon frames provide basic information about the AP
  - Timestamps
  - Beacon interval
  - Service Set IDentifier (SSID)
  - Capability info including encryptions, data rates supported by the AP
  - Optional info elements for vendor-specific features
- Most APs now can suppress the SSID in beacons – stealth beacons
  - Some people suggest this increases WLAN security
  - However, the SSID is still transmitted when an AP and a STA get connected

SSID & STA Probe

- The SSID is just a name made for each wireless LAN
  - Multiple APs can announce the same SSID
  - STAs will assume the APs are parts of the same network
    - > An STA can be registered with one AP only
- An STA can be configured to actively search for a specific WLAN
  - The STA broadcasts Probe Requests looking for a specific SSID through one or more channels
  - AP(s) with the matching SSID reply with Probe Response messages

STA – AP Connection



Two-phase process to get connected

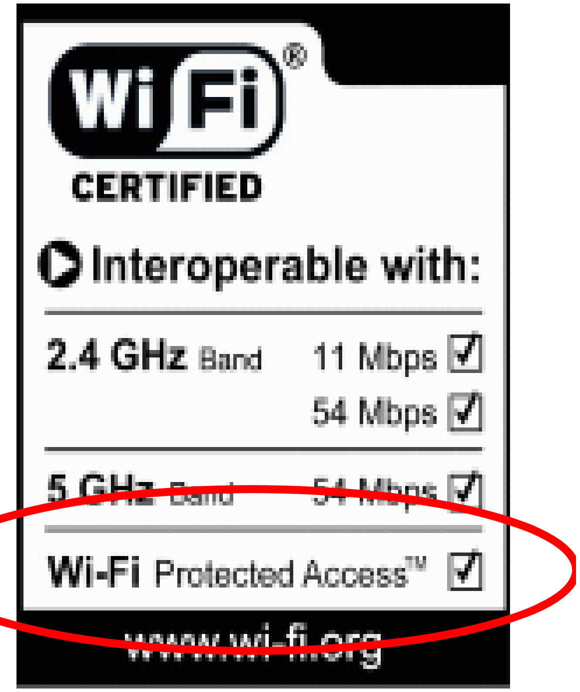
- Authentication options
  - Open System: only use STA's MAC address to "authenticate"
  - Shared Key: performing challenging-response exchange
- Association with agreed connection parameters
  - Data rate
  - Encryption
  - The SSID, …

Problems with 802.11 WEP

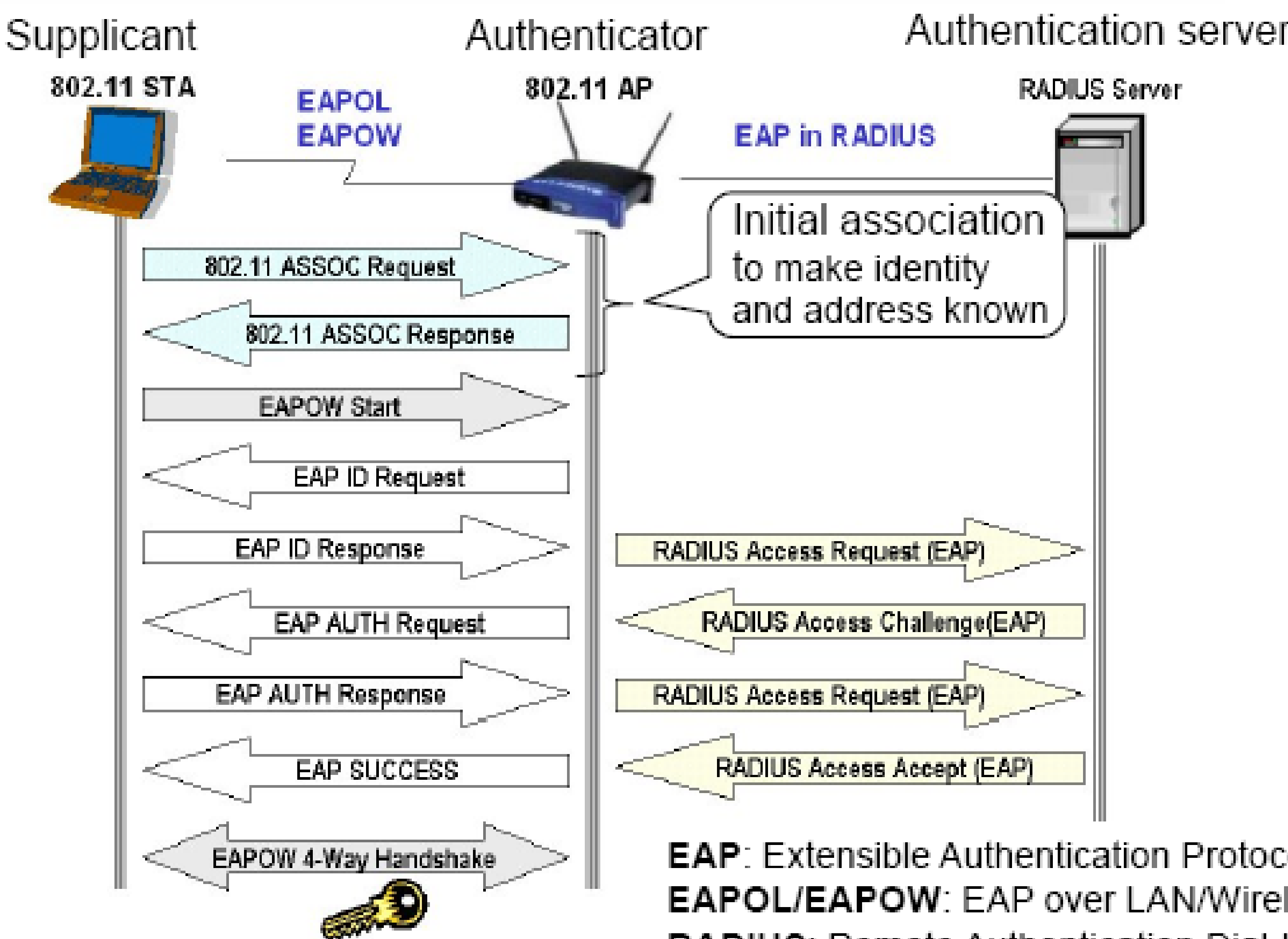
- 802.11 suggests Wired Equivalent Privacy (WEP) encryption
  - In three possible modes: No encryption, 40 or 128 bit WEP encryption
  - WEP uses the RC4 stream cipher to encrypt a TCP/IP packet by XOR-ing it with a key-stream
  - Keys generated by a 24 bit Initialization Vector (IV)
- WEP cannot be trusted for security because it frequently repeats RC4 IVs
  - Attackers can eavesdrop, spoof wireless traffic
  - Attack tools are available for download and capable to break the key with a few minutes of traffic
- WEP is not often used in large wireless networks
  - High administrative costs on key mgmt
  - Not usable for enterprise WLAN with lots of wireless stations

Wi-Fi Protected Access (WPA)

- A certification program developed to replace WEP by the Wi-Fi Alliance – a global industry association
  - Software upgrade to existing hardware
  - Forward-compatible with 802.11i
- Better encryption key management: Temporal Key Integrity Protocol (TKIP) with 48-bits IV
- Better message integrity: Michael to protects against forgery attacks
- Improved Authentication:
  - 802.1x and EAP (Extensible Authentication Protocol, per RFC 3748)
  - Mutual authentication, a.k.a. 2WAY authentication

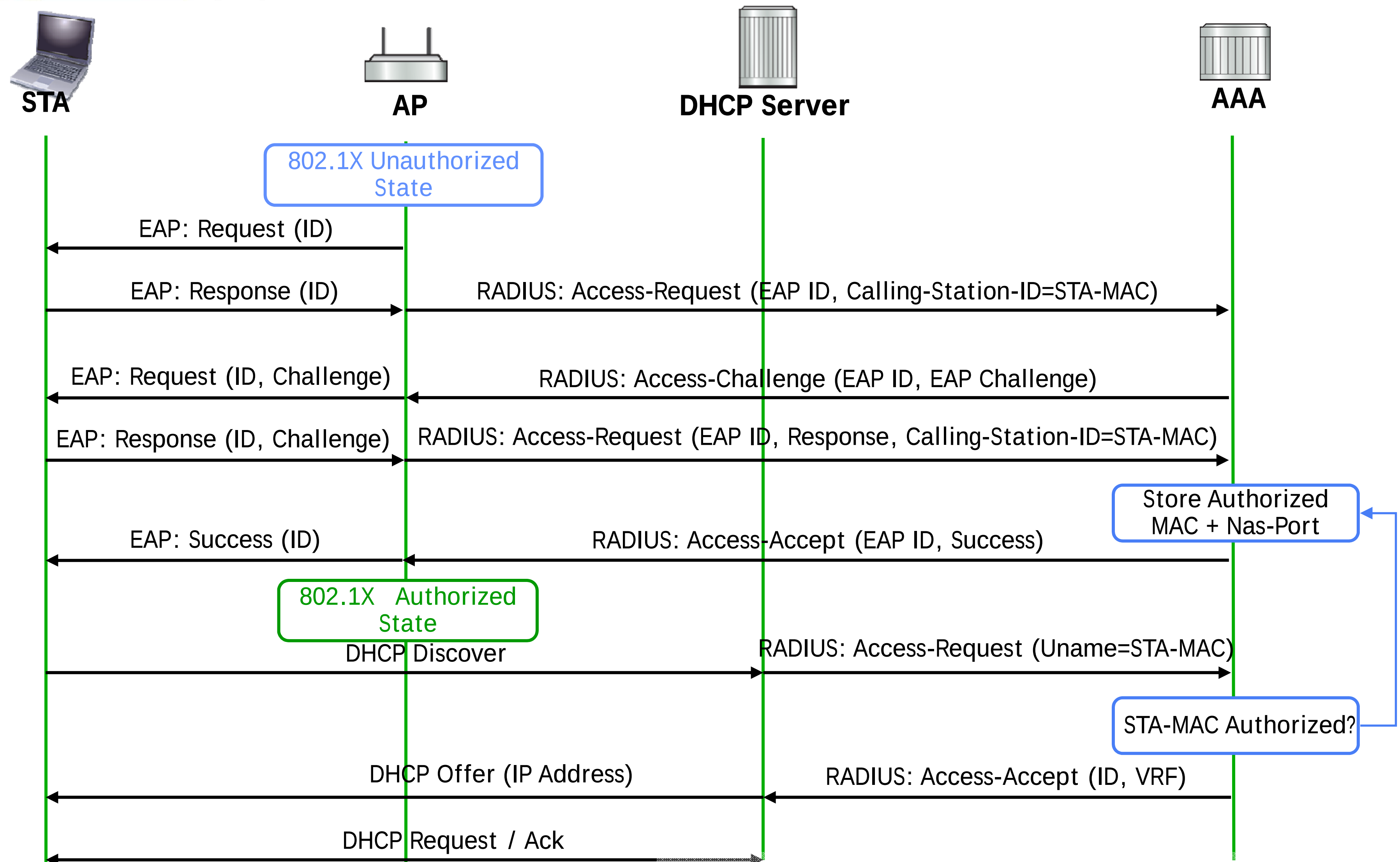


EAPOL/EAPOW Authentication



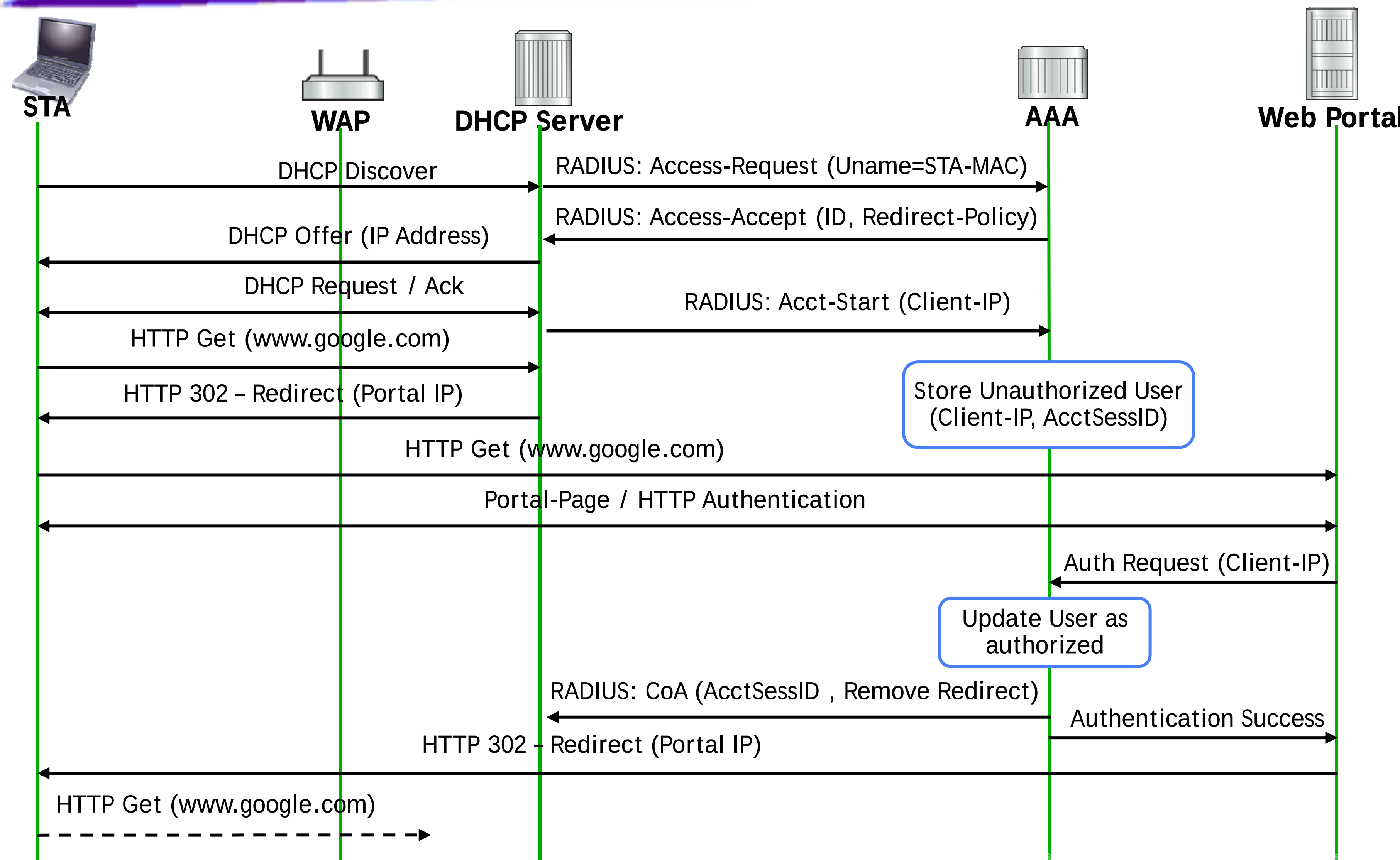
EAP: Extensible Authentication Protocol
EAPOL/EAPOW: EAP over LAN/Wireless
RADIUS: Remote Authentication Dial-In User Service protocol

WLAN Authentication
802.1x & EAP Authentication Call Flow



RADIUS: Remote Authentication Dial In User Service

WLAN Authentication
Web Portal based Authentication Call Flow



RADIUS: Remote Authentication Dial In User Service