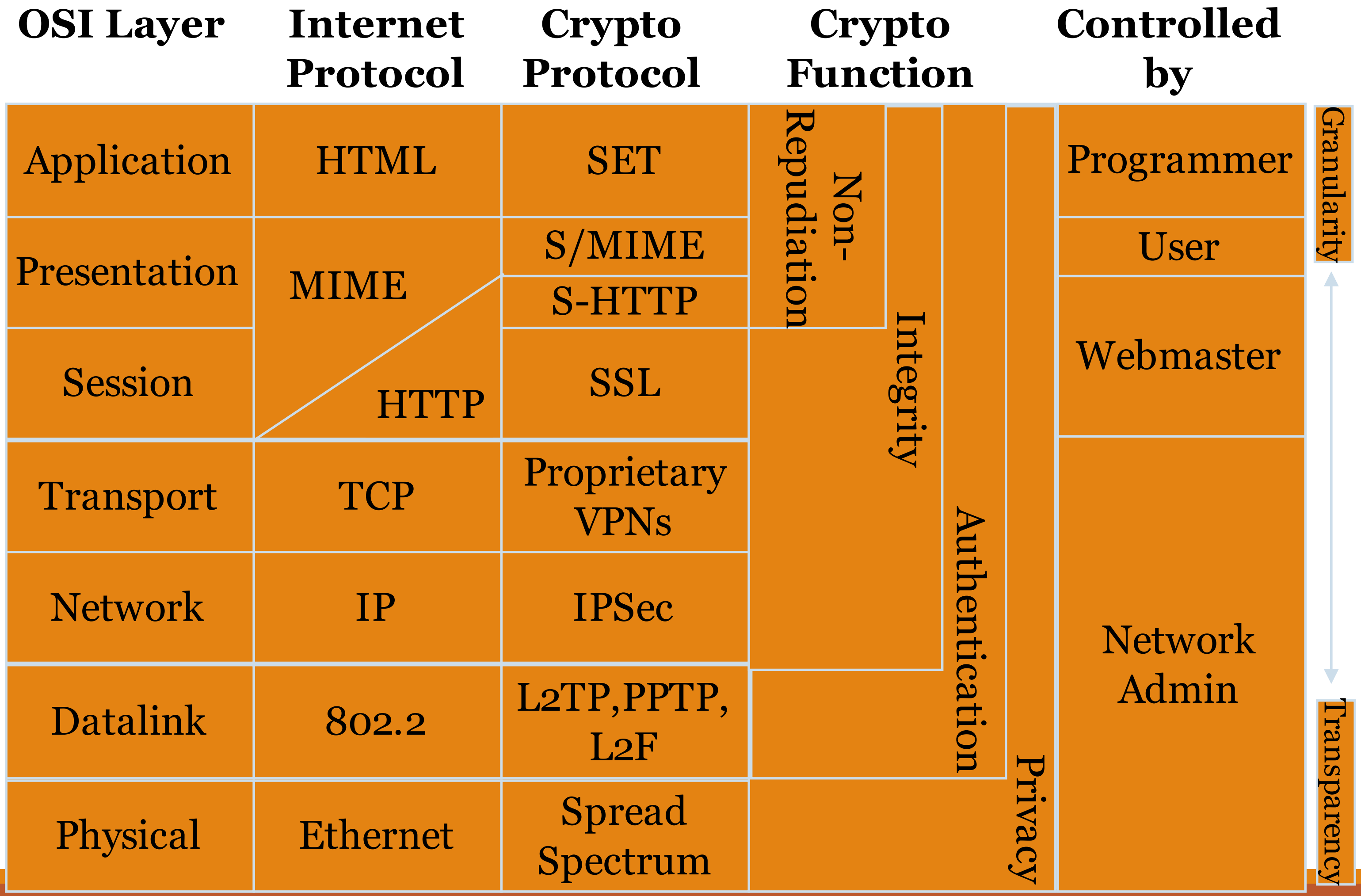
Week 2 – Network Basics

Networking Security

OSI Model Diagram

Excerpt from Information Security Management Handbook, 4th Edition



OSI Layer	Internet Protocol	Crypto Protocol	Crypto Function	Controlled by
Application	HTML	SET	Non-Repudiation Integrity Authentication Privacy	Programmer
Presentation	MIME	S/MIME S-HTTP		User Webmaster
Session	HTTP	SSL		
Transport	TCP	Proprietary VPNs		Network Admin
Network	IP	IPSec		
Datalink	802.2	L2TP,PPTP, L2F		
Physical	Ethernet	Spread Spectrum		

Granularity

Transparency

Open System Interconnect (OSI) Model

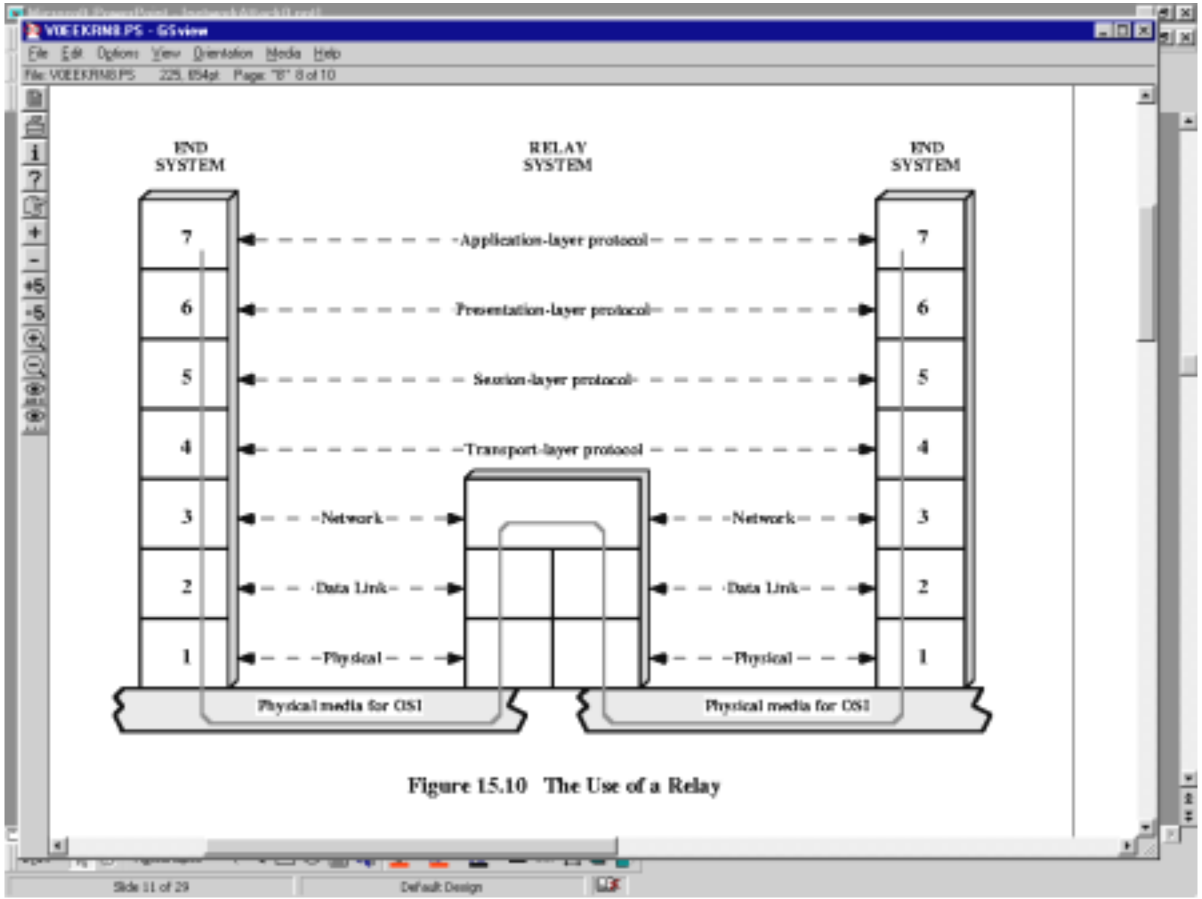
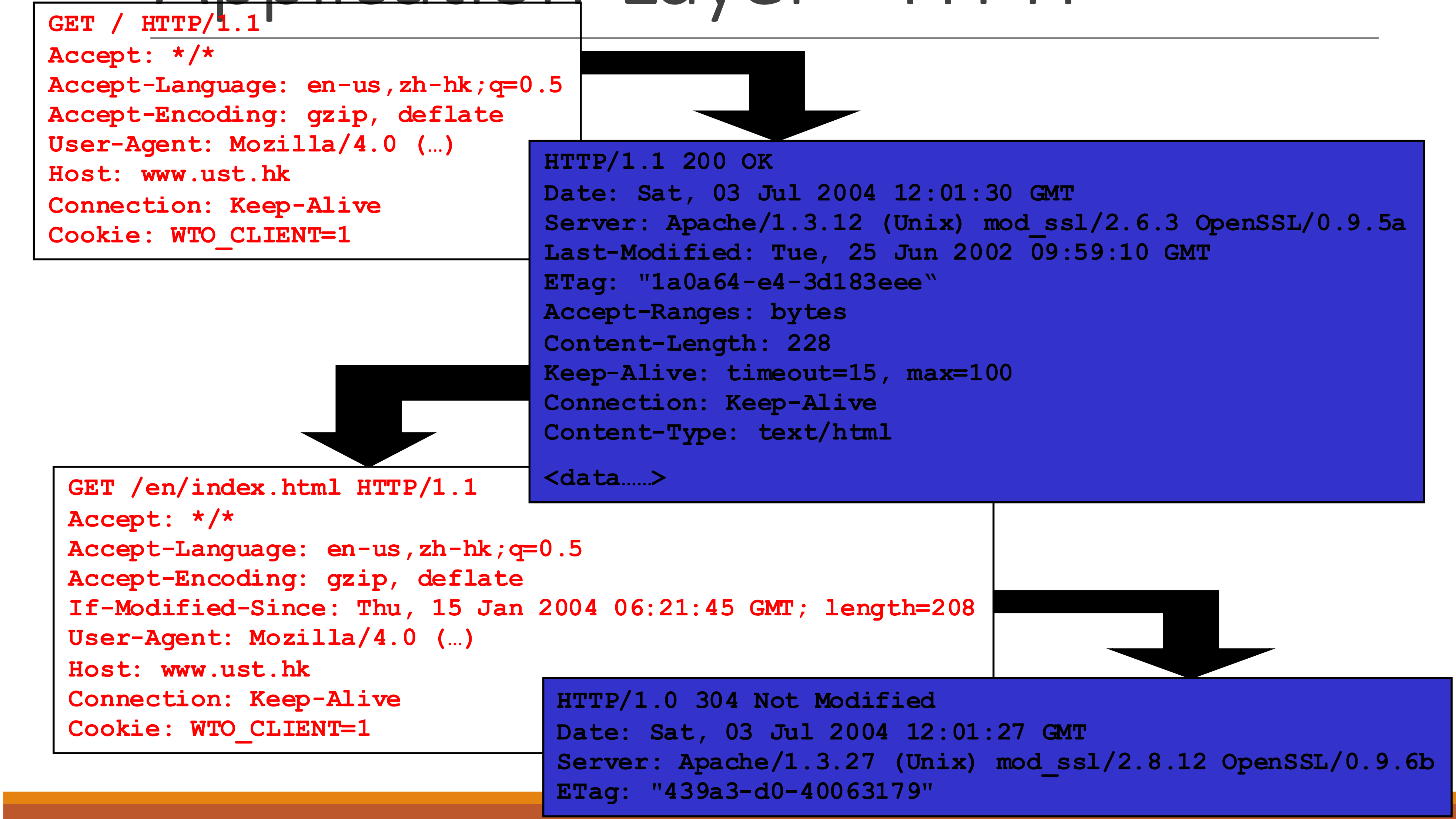


Figure 15.10 The Use of a Relay

Application Layer - HTTP



```
GET / HTTP/1.1
Accept: */*
Accept-Language: en-us,zh-hk;q=0.5
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (…)
Host: www.ust.hk
Connection: Keep-Alive
Cookie: WTO_CLIENT=1
```

```
HTTP/1.1 200 OK
Date: Sat, 03 Jul 2004 12:01:30 GMT
Server: Apache/1.3.12 (Unix) mod_ssl/2.6.3 OpenSSL/0.9.5a
Last-Modified: Tue, 25 Jun 2002 09:59:10 GMT
ETag: "1a0a64-e4-3d183eee“
Accept-Ranges: bytes
Content-Length: 228
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text/html

<data……>
```

```
GET /en/index.html HTTP/1.1
Accept: */*
Accept-Language: en-us,zh-hk;q=0.5
Accept-Encoding: gzip, deflate
If-Modified-Since: Thu, 15 Jan 2004 06:21:45 GMT; length=208
User-Agent: Mozilla/4.0 (…)
Host: www.ust.hk
Connection: Keep-Alive
Cookie: WTO_CLIENT=1
```

```
HTTP/1.0 304 Not Modified
Date: Sat, 03 Jul 2004 12:01:27 GMT
Server: Apache/1.3.27 (Unix) mod_ssl/2.8.12 OpenSSL/0.9.6b
ETag: "439a3-d0-40063179"
```

Application Layer - SMTP

```
220 imsmq09.netvigator.com ESMTP Sendmail 8.12.10/8.12.10; Sat, 3 Jul 2004 20:17:39 +0800

HELO DEMO

250 imsmq09.netvigator.com Hello pcd633218.netvigator.com [218.102.165.218], pleased to
 meet you

MAIL FROM: <sender@netvigator.com>

250 2.1.0 <sender@netvigator.com>... Sender ok

RCPT TO: <receiver@cs.ust.hk>

250 2.1.5 <receiver@cs.ust.hk>... Recipient ok

RSET

250 2.0.0 Reset state

MAIL FROM: <sender@netvigator.com>

250 2.1.0 <sender@netvigator.com>... Sender ok

RCPT TO: <receiver@cs.ust.hk>

250 2.1.5 <receiver@cs.ust.hk>... Recipient ok

DATA

354 Enter mail, end with "." on a line by itself
```

Presentation Layer – SMTP

```
Message-ID:
 <006f01c460f7$bbf3c440$6401a8c0@Jeep>

From: "Sender" <sender@netvigator.com>

To: "Receiver" <receiver@cs.ust.hk>

Subject: Demo

Date: Sat, 3 Jul 2000 20:17:36 +0800

MIME-Version: 1.0

Content-Type: multipart/mixed;

 boundary="----
 =_NextPart_000_006C_01C4613A.C7BFF4E0"



This is a multi-part message in MIME format.



------=_NextPart_000_006C_01C4613A.C7BFF4E0

Content-Type: text/plain;

 charset="big5"

Content-Transfer-Encoding: 7bit
```

```
------=_NextPart_000_006C_01C4613A.C7BFF4E0

Content-Type: image/bmp;

 name="my tiredness graph.BMP"

Content-Transfer-Encoding: base64

Content-Disposition: attachment;

 filename="my tiredness graph.BMP"



Qk1KlgAAAAAAAEoAAAAoAAAAfAEAAMgAAAABAAQAAAAA
 AAAAAAB0EgAAdBIAAAUAAAAFAAAA////

… … …

------=_NextPart_000_006C_01C4613A.C7BFF4E0-
 -
```

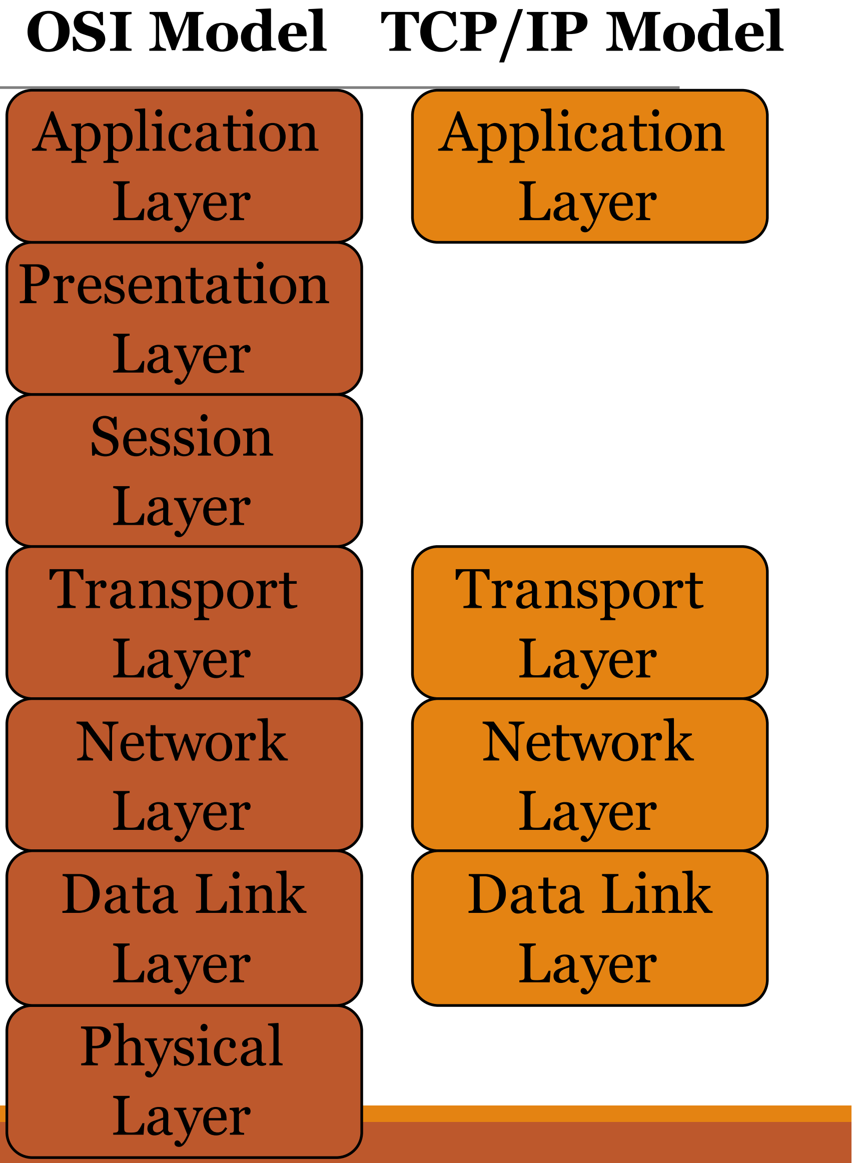
Session Layer – SSL

```
CONNECTED(00000790)

depth=2 /C=US/O=VeriSign, Inc./OU=Class 3 Public Primary Certification Authority


Certificate chain

  … … …

Server certificate

  … … …

No client certificate CA names sent

SSL handshake has read 2769 bytes and written 330 bytes

---

New, TLSv1/SSLv3, Cipher is RC4-MD5

Server public key is 1024 bit

SSL-Session:

    Protocol  : TLSv1

    Cipher    : RC4-MD5

    Session-ID: 0000E554D99EB7AA58585858585858585858585858585858585840E6A6CA00000285

    Session-ID-ctx:

    Master-Key: D708B9C625E3183AE8E48D18723BE2ECE0E73F6A366283D07A34D69604D1AA15........
```

TCP/IP Model

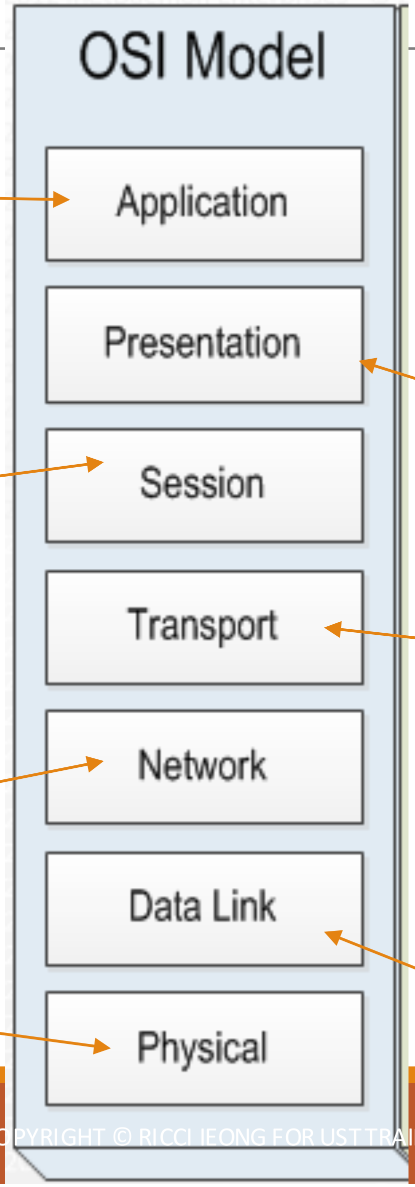
defines only 4 layers:

- Application Layer
  - FTP, HTTP, DNS, SMTP, …
- Host-to-Host Transport Layer
  - TCP, UDP
- Internet Layer
  - IP, ARP, RARP, ICMP
- Network Link Layer
  - Ethernet, FastEthernet, SLIP, PPP



OSI Model	TCP/IP Model
Application Layer	Application Layer
Presentation Layer	
Session Layer	
Transport Layer	Transport Layer
Network Layer	Network Layer
Data Link Layer	Data Link Layer
Physical Layer	

Attacks on each layer in OSI model



- Buffer Overflow
- SQL Injection
- Authentication Brute Force

- SSL DoS
- SSL MITM

- Session Hijacking
- DNS Poisoning

- TCP Flooding
- UDP Flooding

- Ping Flood
- Port scanning
- Fingerprinting

- Packet sniffing
- MAC Address Spoofing
- VLAN Attack
- ARP Cache Poisoning

Keystroke Logging

Lockpicking

Cutting Cable

What is LAN

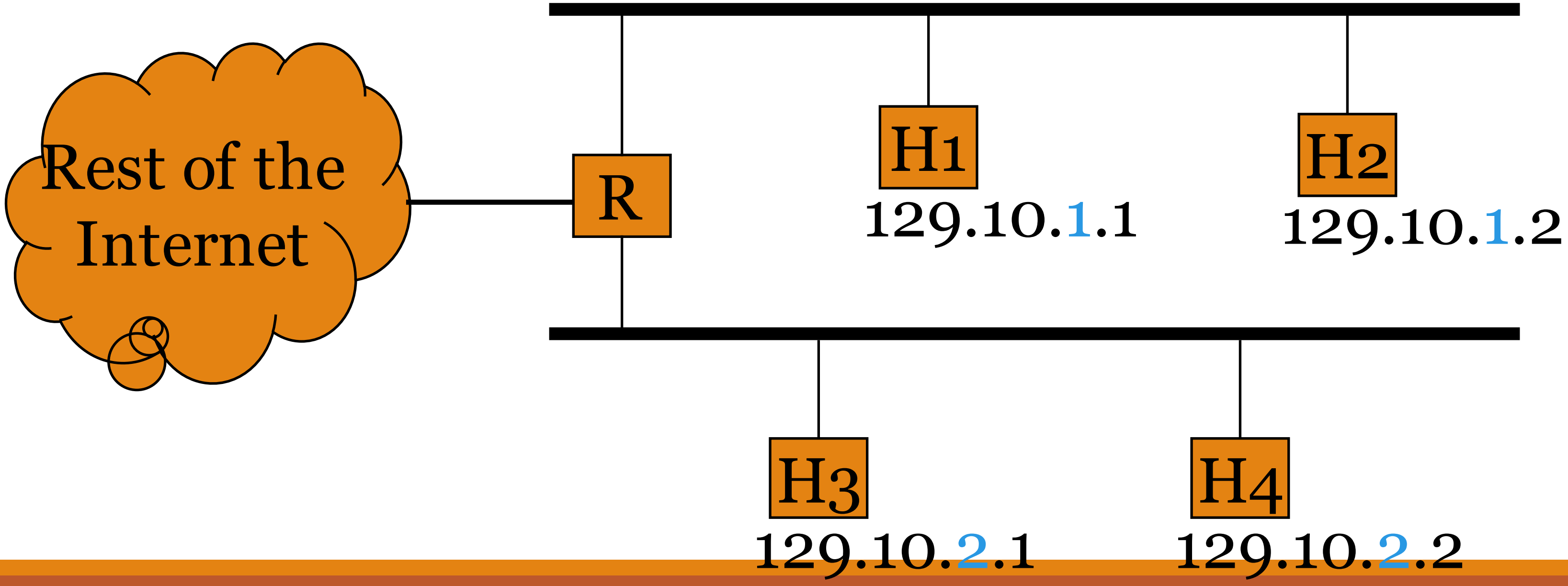
Local area network (LAN)

- a group of computers and associated devices that share a common communications line or wireless link and typically share the resources of a single processor or server within a small geographic area
- Major local area network technologies are:
  - Ethernet
  - Token Ring
  - FDDI (Fiber Distributed Data Interface)

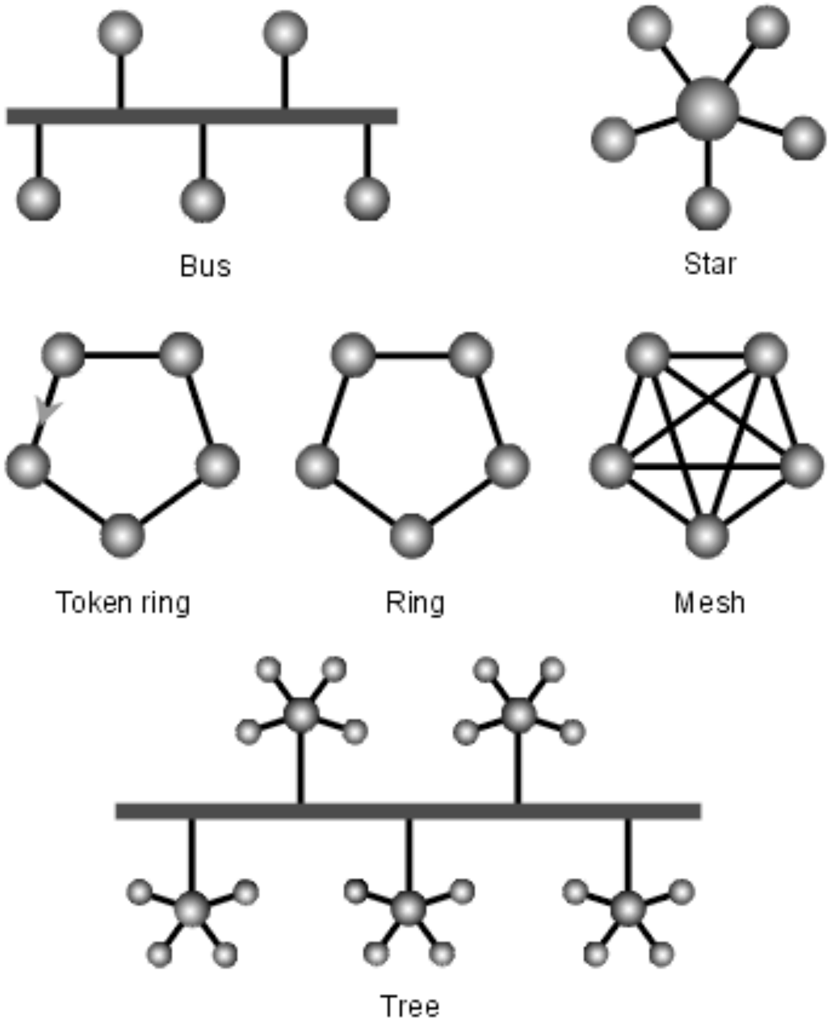
Subnetting

Router routes packets to the appropriate subnet from outside

implemented by subnet masks



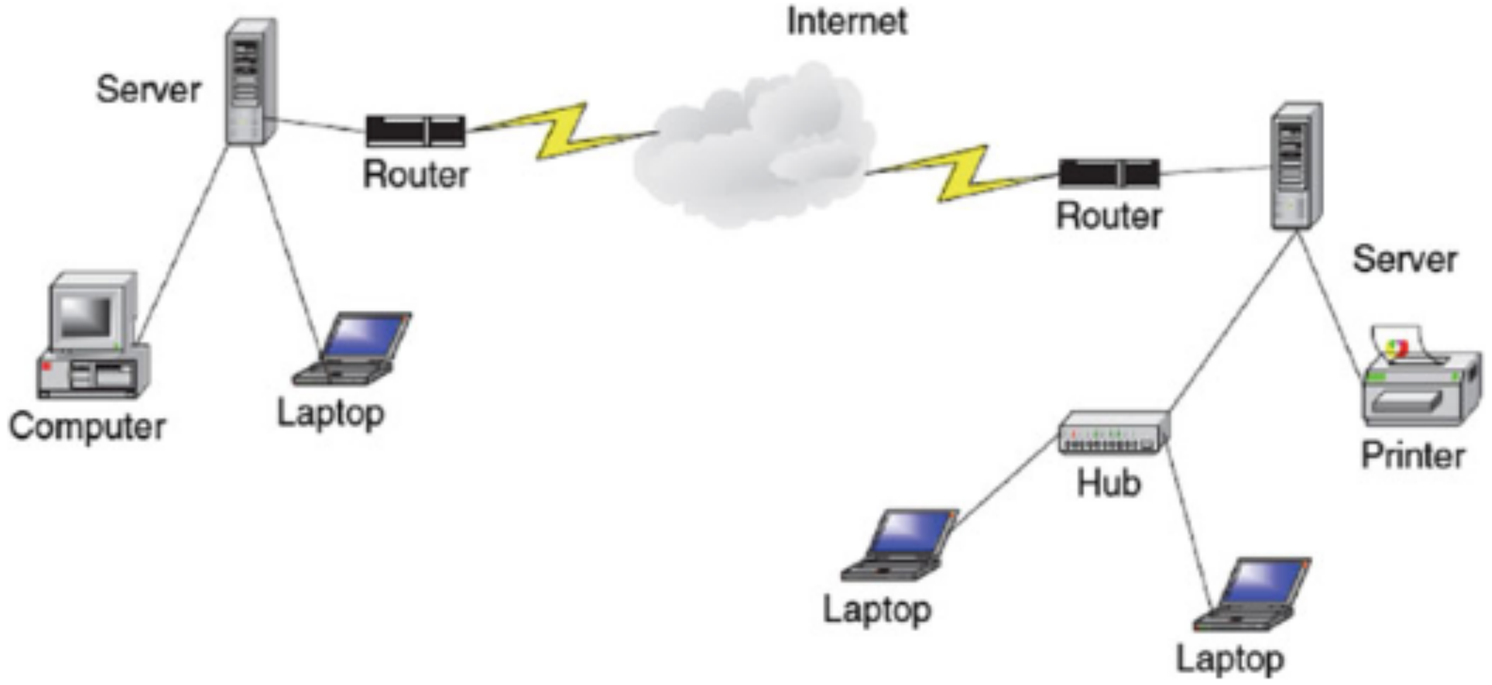
Network Topology



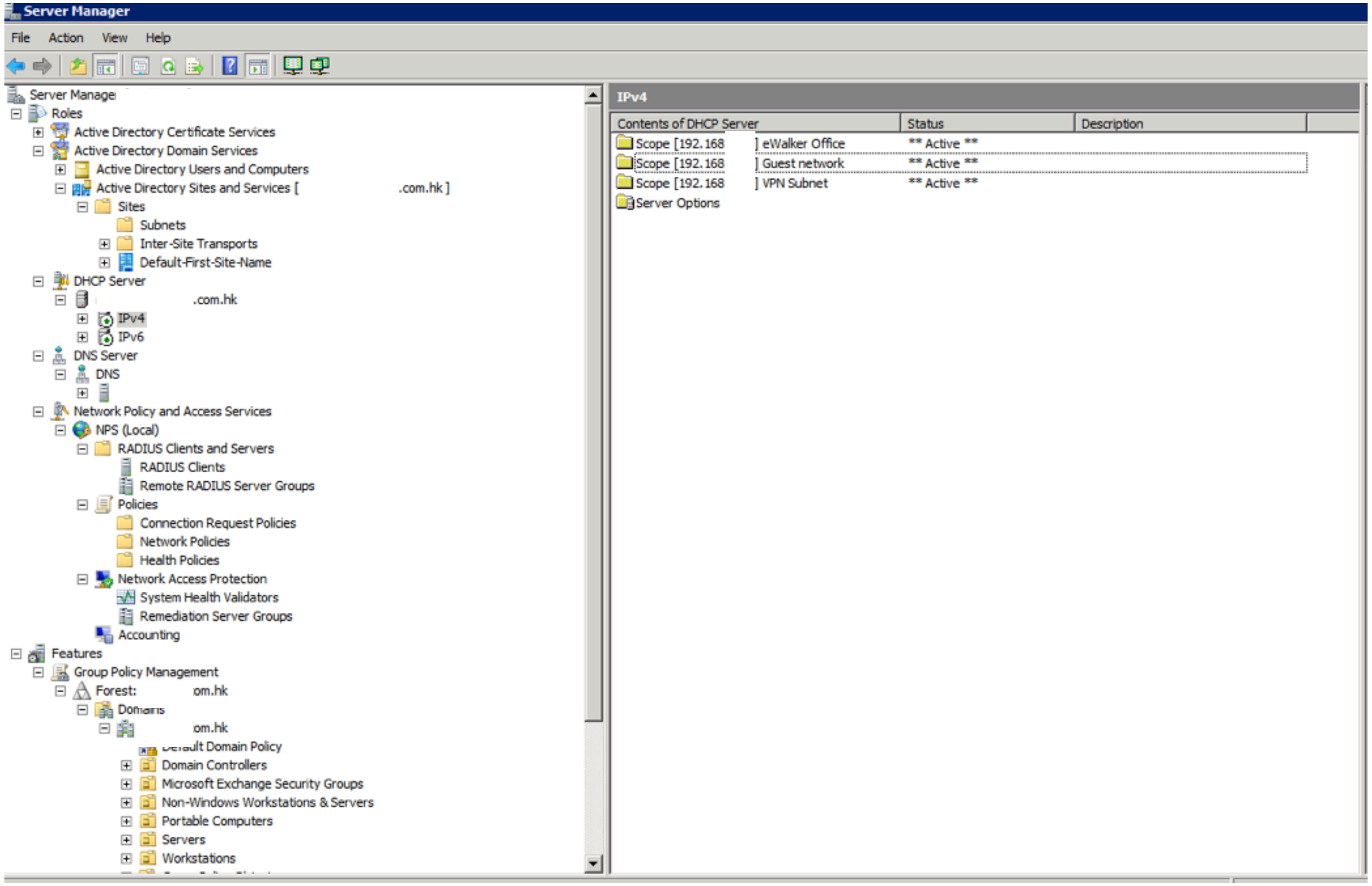
What is WAN

Span broad geographical distances

Consists of combination of switched and dedicated lines, microwave and satellite communications



Network Access Protection (NAP) in Windows environment



- Server Manage
  - Roles
    - Active Directory Certificate Services
    - Active Directory Domain Services
      - Active Directory Users and Computers
      - Active Directory Sites and Services [.com.hk]
        - Sites
          - Subnets
          - Inter-Site Transports
          - Default-First-Site-Name
    - DHCP Server
      - .com.hk
        - IPv4
        - IPv6
    - DNS Server
      - DNS
    - Network Policy and Access Services
      - NPS (Local)
        - RADIUS Clients and Servers
          - RADIUS Clients
          - Remote RADIUS Server Groups
        - Policies
          - Connection Request Policies
          - Network Policies
          - Health Policies
        - Network Access Protection
          - System Health Validators
          - Remediation Server Groups
        - Accounting
  - Features
    - Group Policy Management
      - Forest: om.hk
        - Domains
          - om.hk
            - Default Domain Policy
            - Domain Controllers
            - Microsoft Exchange Security Groups
            - Non-Windows Workstations & Servers
            - Portable Computers
            - Servers
            - Workstations

Contents of DHCP Server	Status	Description
Scope [192.168] eWalker Office	** Active **	
Scope [192.168] Guest network	** Active **	
Scope [192.168] VPN Subnet	** Active **	
Server Options		

Network Architecture

Security from layered approach

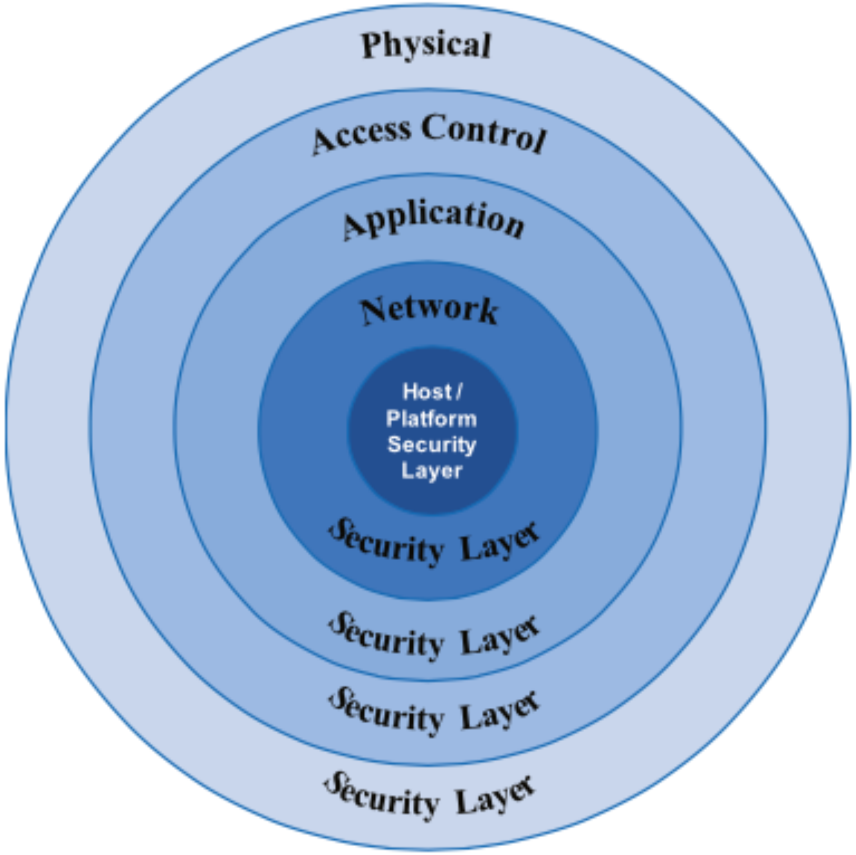
Standards

Policy

Procedures

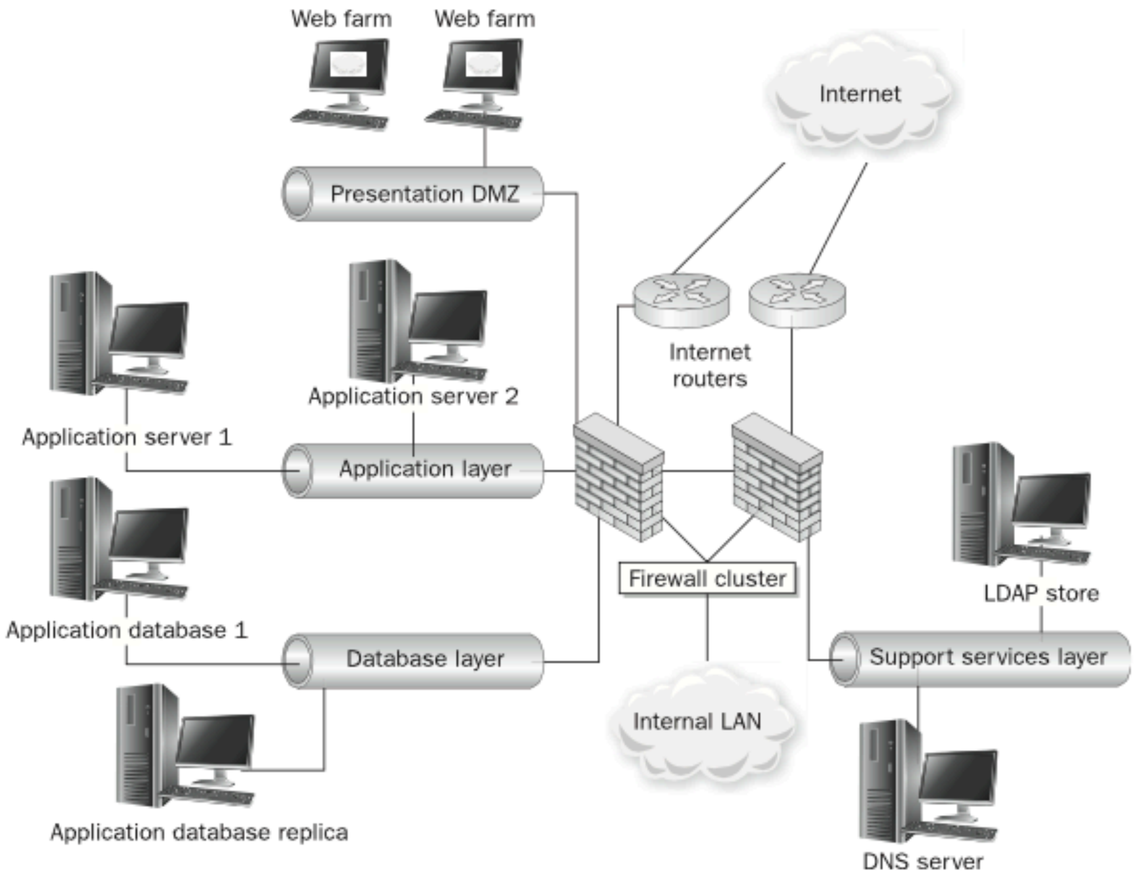
Controls

Constructive Security



From The InfoSec Handbook (2014)

Typical Web and Mobile application



Example of multi-tier application infrastructure from "Information Security The Complete Reference, 2nd Edition"

Web Server

Characteristics of Web Server

- Use Information technology
- Process requests via HTTP protocol
- Distribute information on the World Wide Web
- Via user agent – Web Browser

Support server-side scripting

- PHP
- Active Server Pages

Support browser-side scripting

- Java
- JavaScript

First Web Server in 1989

Database Server

Characteristics of Database Server

- Defined by the client-server model and provides database services to other computer programs
- Works with Query language
- e.g. MySQL, Oracle, DB2, Informix, M

Security Architecture (Example) – X.800

X.800 defines a security service as a service that is provided by a protocol layer of communicating open systems and that ensures adequate security of the systems or of data transfers.

Five categories of services	14 specific services
Authentication	1. Peer Entity Authentication 2. Data-Origin Authentication
Access Control	1. Access Control
Data Confidentiality	1. Connection Confidentiality 2. Connectionless Confidentiality 3. Selective-Field Confidentiality 4. Traffic-Flow Confidentiality
Data Integrity	1. Connection Integrity with Recovery 2. Connection Integrity without Recovery 3. Selective-Field Connection Integrity 4. Connectionless Integrity 5. Selective-Field Connectionless Integrity
Non-Repudiation	1. Non-Repudiation, Origin 2. Non-Repudiation, Destination

How can we connect to a web site

Domain Name System (DNS)

Application Layer, Connectionless

- Usually look up names to IP addresses (forward lookup)

RFC 1034, RFC 1035

Consists of domain names, name servers and DNS records

Can be overridden locally

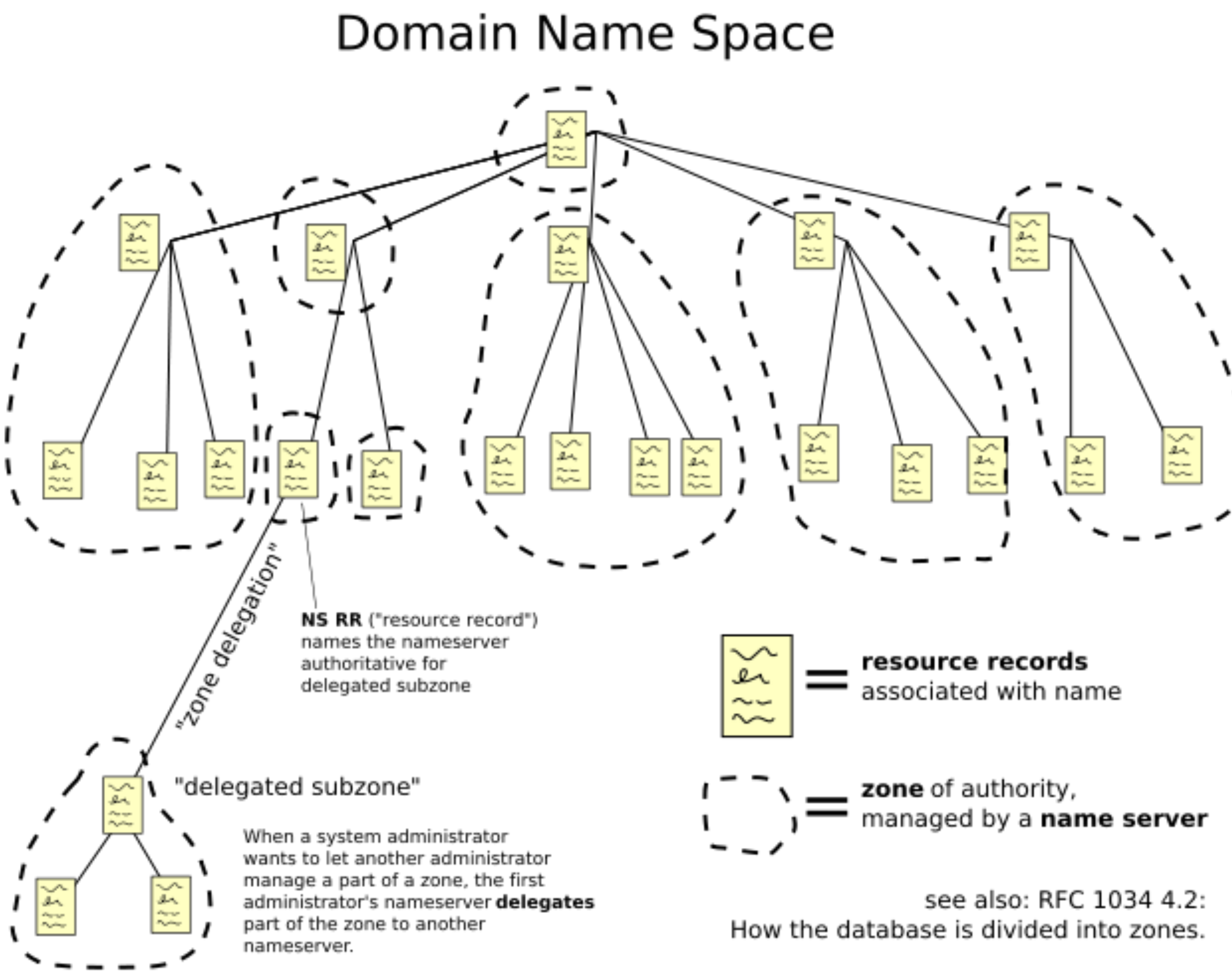
- Some viruses denied signature update with this

Growing attacks against the DNS architecture

DNS Protocol Format

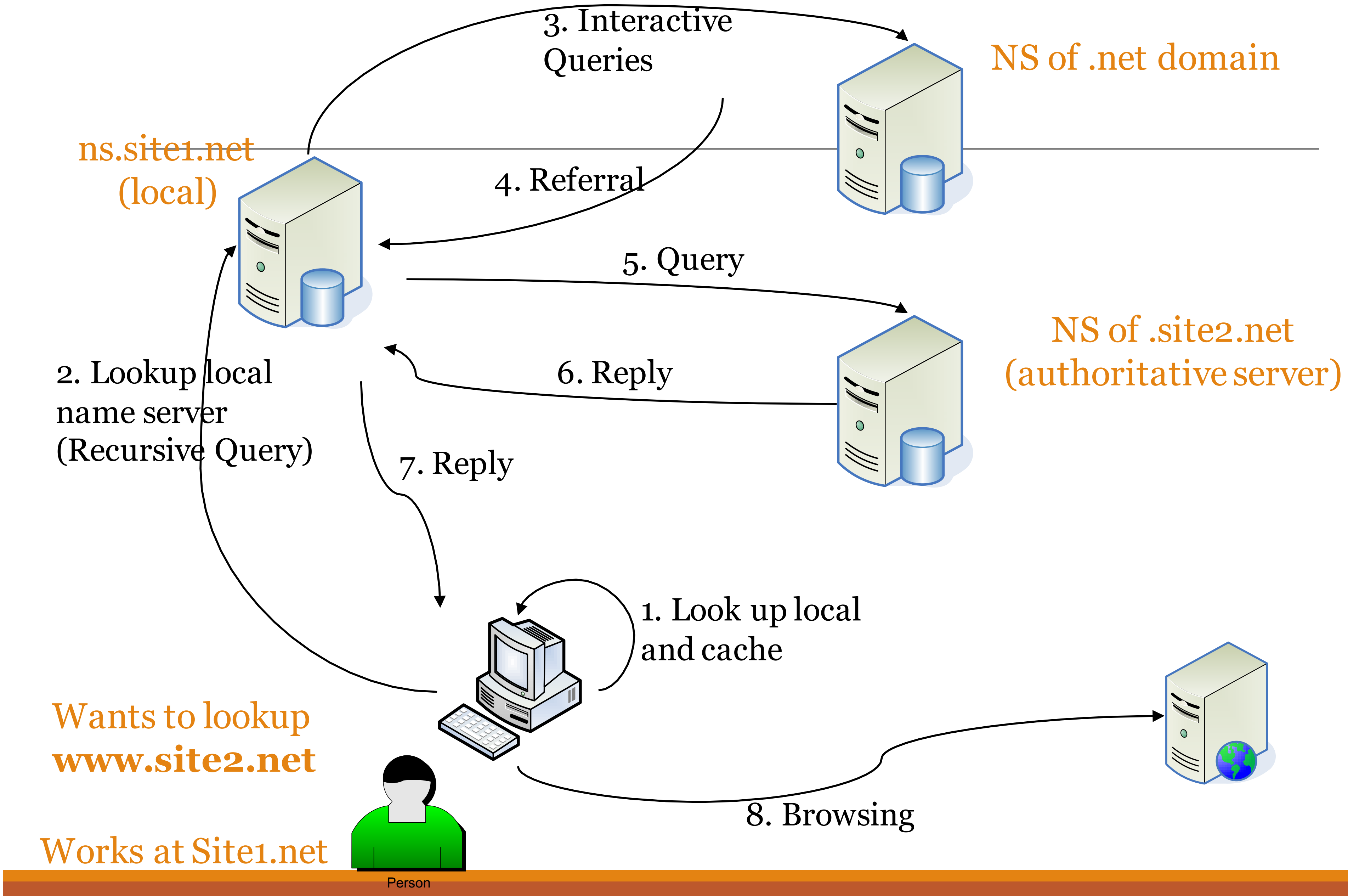
ID	Flags
Number of questions	Numbers of answers
Number of RR authority	Number of supplementary RR
Question	
Answer	
Additional information	

DNS

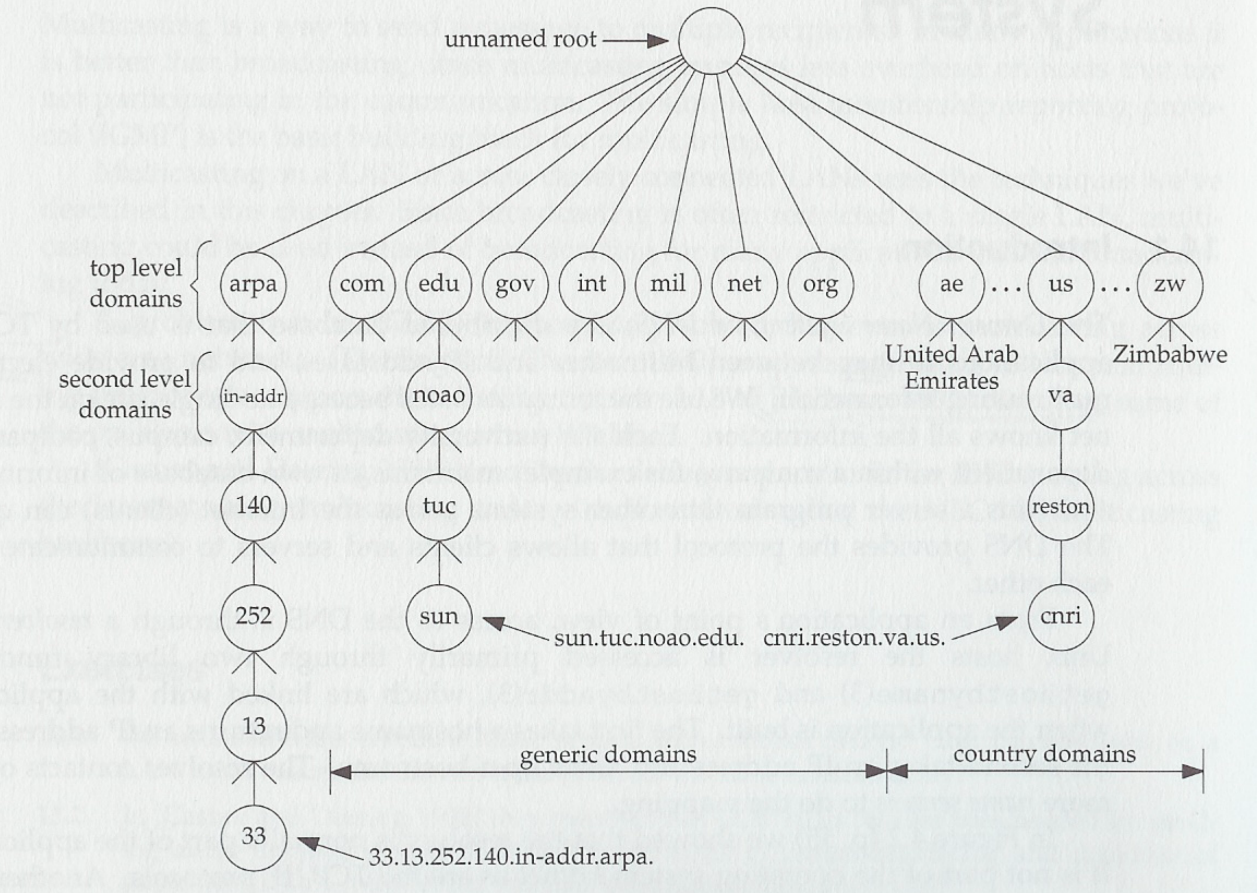

Domain Name Space
"zone delegation"
NS RR ("resource record") names the nameserver authoritative for delegated subzone
"delegated subzone"
When a system administrator wants to let another administrator manage a part of a zone, the first administrator's nameserver **delegates** part of the zone to another nameserver.
= **resource records** associated with name
= **zone** of authority, managed by a **name server**
see also: RFC 1034 4.2: How the database is divided into zones.

By LionKimbro

DNS operation illustration


3. Interactive Queries
NS of .net domain
ns.site1.net (local)
4. Referral
5. Query
NS of .site2.net (authoritative server)
2. Lookup local name server (Recursive Query)
6. Reply
7. Reply
1. Look up local and cache
Wants to lookup **www.site2.net**
8. Browsing
Works at Site1.net
Person

DNS Architecture

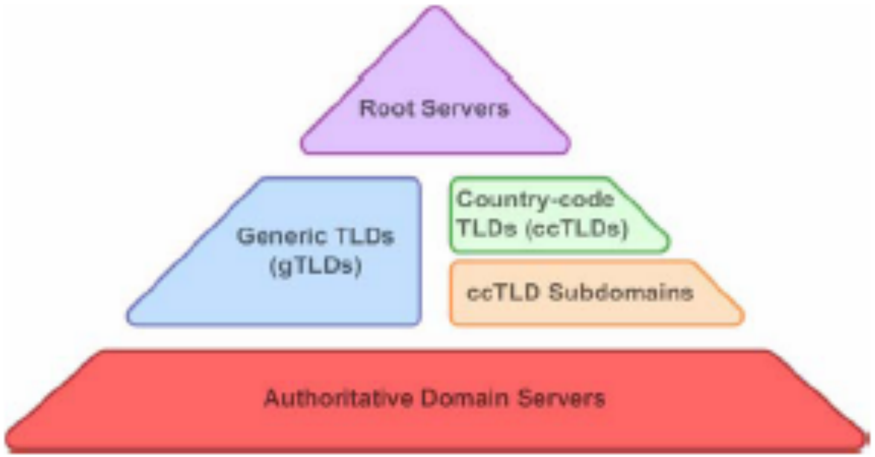


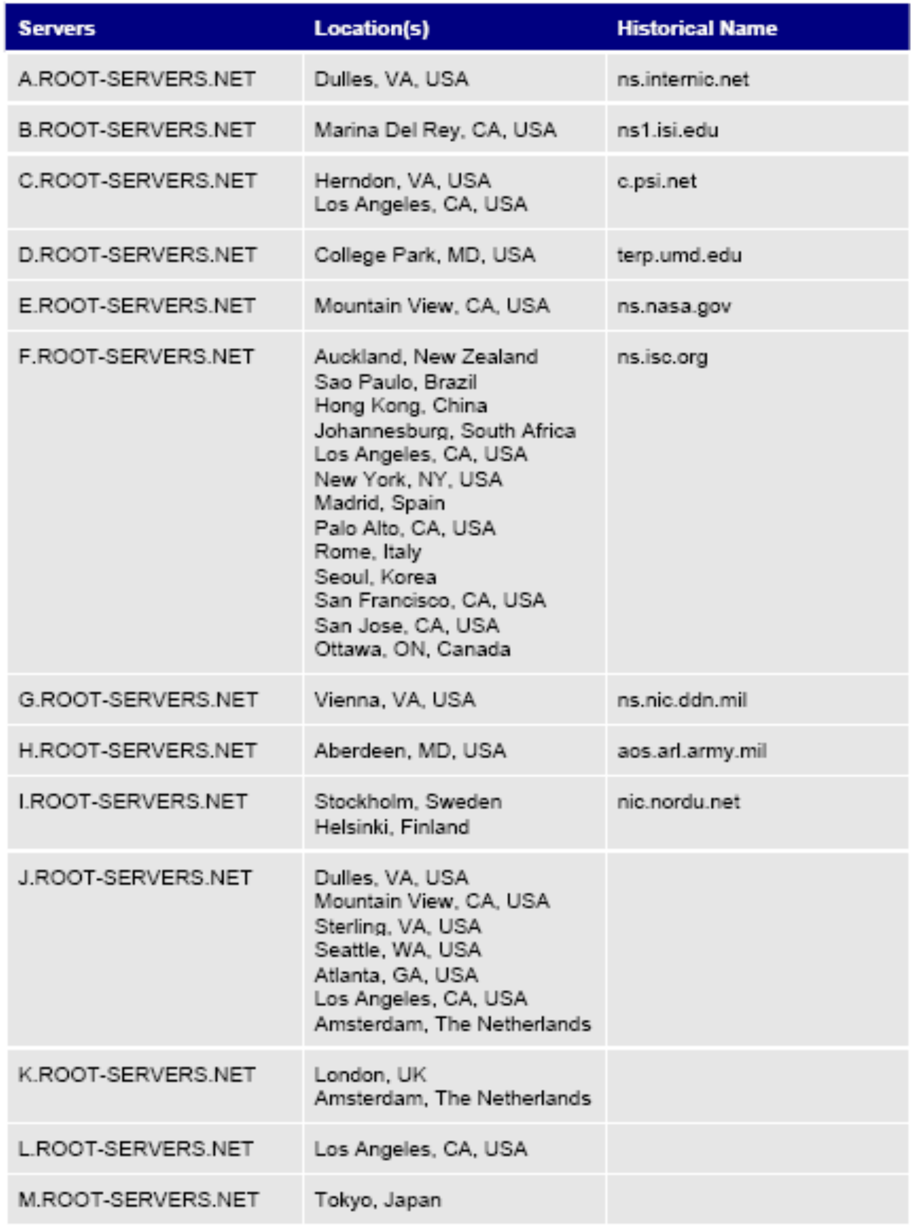
DNS Architecture (Cont.)

Domain names registration

- InterNIC
  - http://www.internic.net/
- Accredited registrars:
  - http://www.internic.net/alpha.html

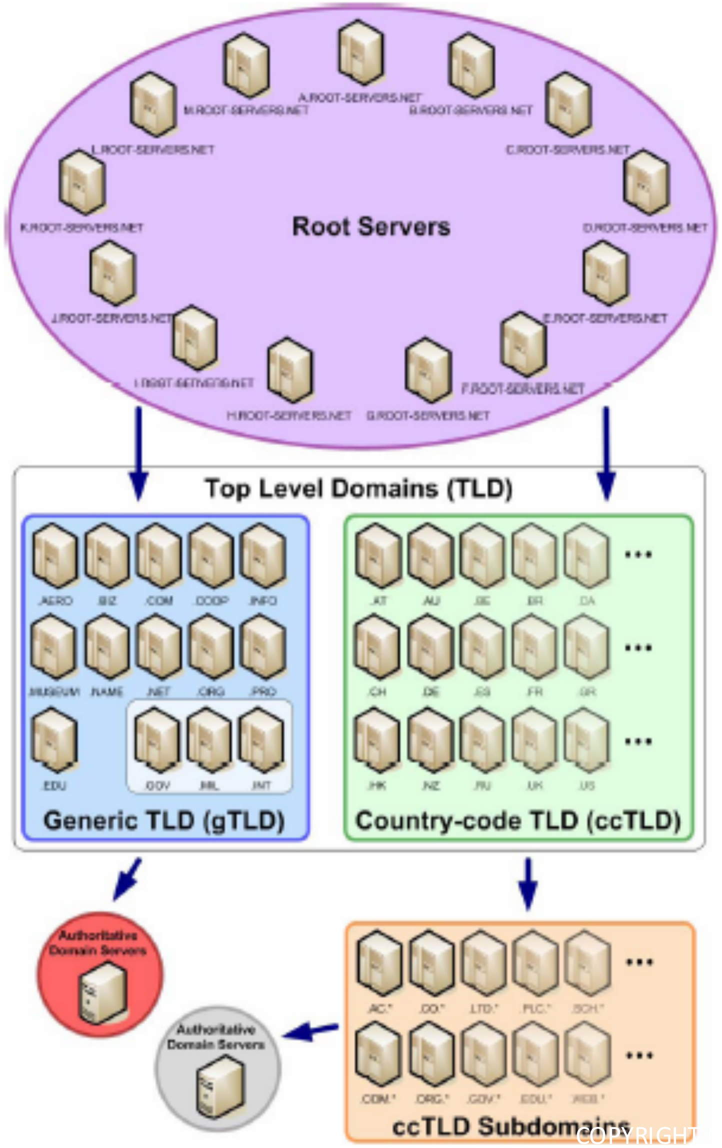
DNS

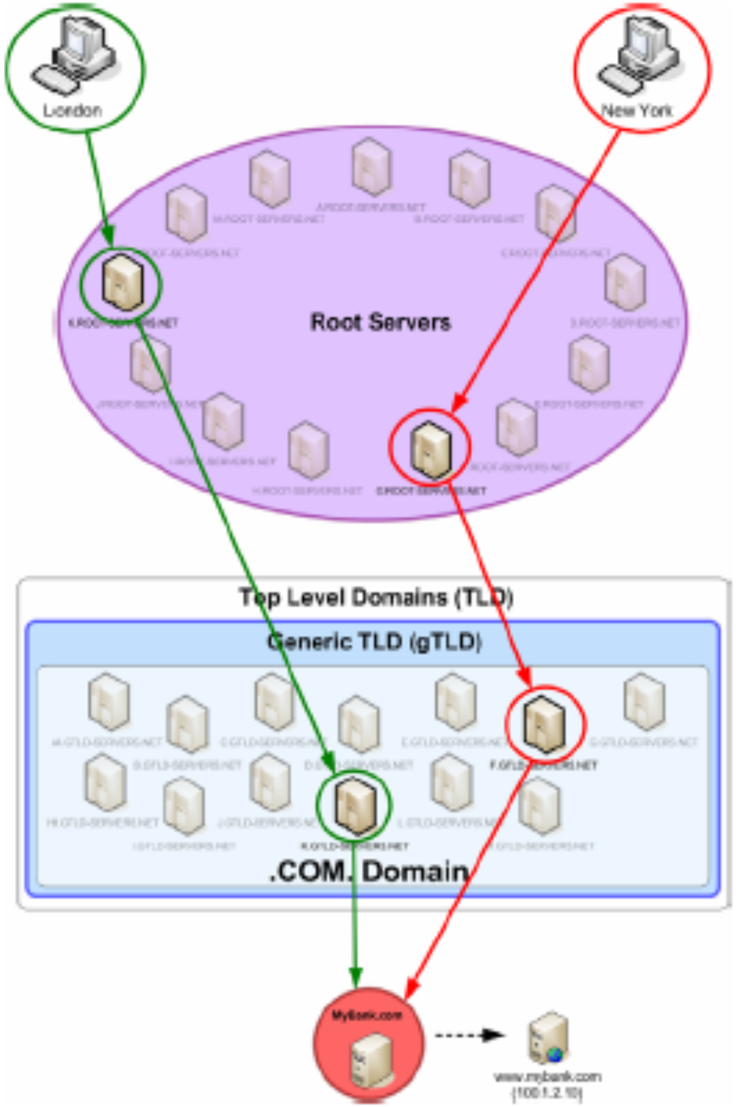




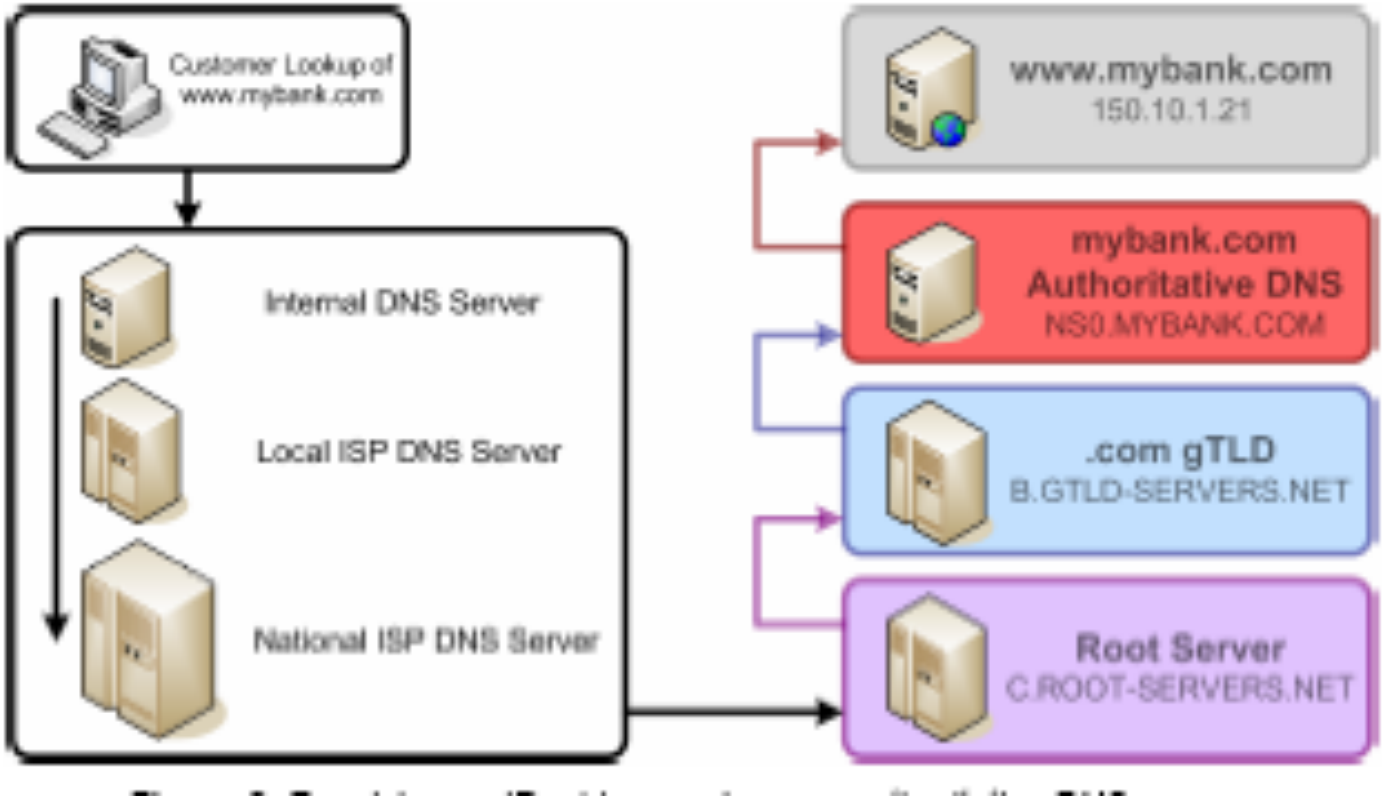
Servers	Location(s)	Historical Name
A.ROOT-SERVERS.NET	Dulles, VA, USA	ns.internic.net
B.ROOT-SERVERS.NET	Marina Del Rey, CA, USA	ns1.isi.edu
C.ROOT-SERVERS.NET	Herndon, VA, USA Los Angeles, CA, USA	c.psi.net
D.ROOT-SERVERS.NET	College Park, MD, USA	terp.umd.edu
E.ROOT-SERVERS.NET	Mountain View, CA, USA	ns.nasa.gov
F.ROOT-SERVERS.NET	Auckland, New Zealand Sao Paulo, Brazil Hong Kong, China Johannesburg, South Africa Los Angeles, CA, USA New York, NY, USA Madrid, Spain Palo Alto, CA, USA Rome, Italy Seoul, Korea San Francisco, CA, USA San Jose, CA, USA Ottawa, ON, Canada	ns.isc.org
G.ROOT-SERVERS.NET	Vienna, VA, USA	ns.nic.ddn.mil
H.ROOT-SERVERS.NET	Aberdeen, MD, USA	aos.arl.army.mil
I.ROOT-SERVERS.NET	Stockholm, Sweden Helsinki, Finland	nic.nordu.net
J.ROOT-SERVERS.NET	Dulles, VA, USA Mountain View, CA, USA Sterling, VA, USA Seattle, WA, USA Atlanta, GA, USA Los Angeles, CA, USA Amsterdam, The Netherlands	
K.ROOT-SERVERS.NET	London, UK Amsterdam, The Netherlands	
L.ROOT-SERVERS.NET	Los Angeles, CA, USA	
M.ROOT-SERVERS.NET	Tokyo, Japan	

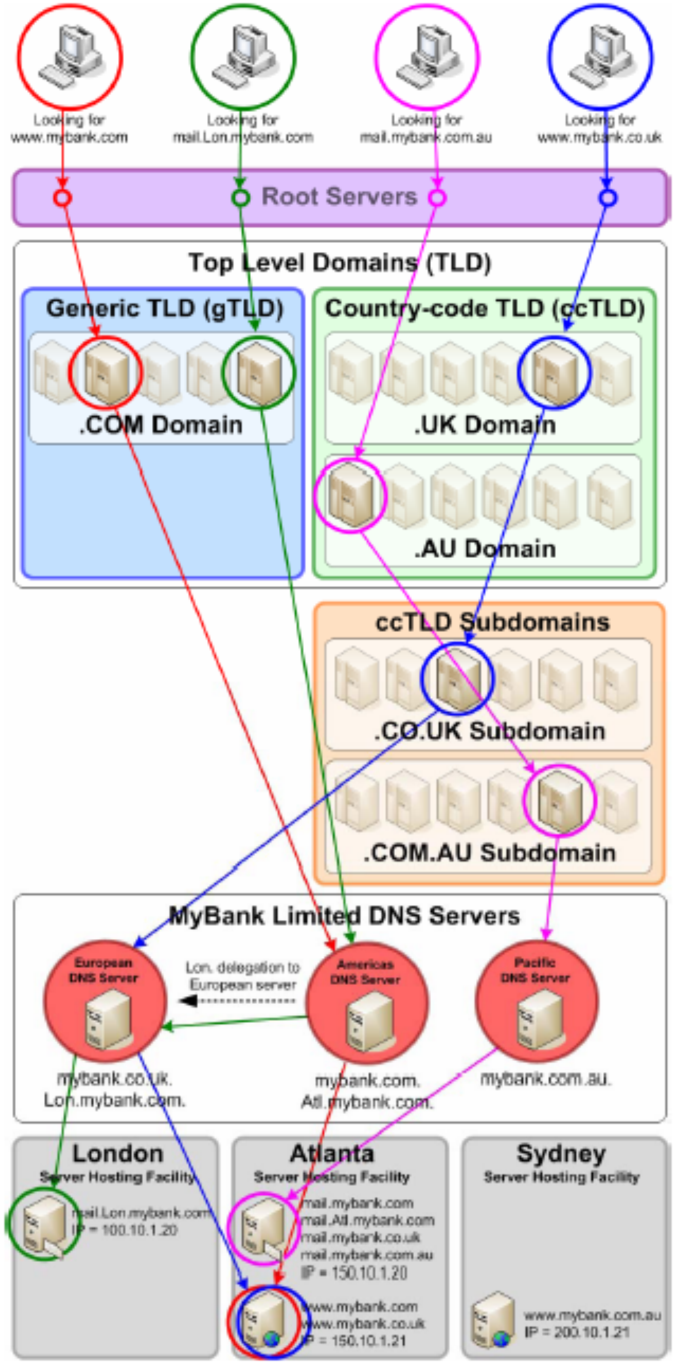
How DNS works





How DNS works




Looking for www.mybank.com
Looking for mail.Lon.mybank.com
Looking for mail.mybank.com.au
Looking for www.mybank.co.uk
Root Servers
Top Level Domains (TLD)
Generic TLD (gTLD)
.COM Domain
Country-code TLD (ccTLD)
.UK Domain
.AU Domain
ccTLD Subdomains
.CO.UK Subdomain
.COM.AU Subdomain
MyBank Limited DNS Servers
European DNS Server
Lon. delegation to European server
Americas DNS Server
Pacific DNS Server
mybank.co.uk.
Lon.mybank.com.
mybank.com.
Atl.mybank.com.
mybank.com.au.
London
Server Hosting Facility
mail.Lon.mybank.com
IP = 100.10.1.20
Atlanta
Server Hosting Facility
mail.mybank.com
mail.Atl.mybank.com
mail.mybank.co.uk
mail.mybank.com.au
IP = 150.10.1.20
www.mybank.com
www.mybank.co.uk
IP = 150.10.1.21
Sydney
Server Hosting Facility
www.mybank.com.au
IP = 200.10.1.21

Web-based check Lab

http://www.checkdomain.com

http://www.traceroute.net

http://www.netcraft.com

http://www.tcpiputils.com

http://www.all-nettools.com/toolbox

http://www.zoneedit.com/lookup.html?ad=whois

http://www.opus1.com/www/traceroute.html

http://shodanhq.com/

http://www.zone-h.org/

http://coffer.com/mac_find/

http://www.nabber.org/projects/geotrace/

Looking Glass

http://lg.eurorings.net/

http://noc.ilan.net.il/LG/

http://lg.cern.ch/

http://www.belwue.de/ueberuns/netz/looking.html

http://drift.uninett.no/cgi-bin/lg.cgi

Intelligence Gathering Online Resources

Entity	Type of Information	Web Site
Electronic Data Gathering, Analysis, and Retrieval system (EDGAR)	System providing companies information pertaining to registration details, periodic reports, and other activities specific to legal aspects	http://www.sec.gov/edgar.shtml
Glass Door/Simply Hired	Online repositories providing information about companies work culture, jobs including salaries, employees reviews, etc.	http://www.glassdoor.com/ | http://www.simplyhired.com/
Name Check/Background Check	Information about usernames and background verification of targets	http://namechk.com/ | http://www.advancedbackg-roundchecks.com/
Central Operations/Robtex	Information about domain names, IP address allocation, and registrars	http://centralops.net | http://www.robtex.com
Intelius	Public records of individuals	http://www.intelius.com/
Jigsaw/LinkedIn	Employees information	http://www.jigsaw.com/ | http://www.linkedin.com/
Spokeo	Personal information such as phone numbers	http://www.spokeo.com/
Hoovers	Corporate information including industry analysis	http://www.hoovers.com/

Intelligence Gathering Online Resources

Entity	Type of Information	Web Site
E-mail Sherlock	Specific e-mail patterns search	http://www.emailsherlock.com/
Pastebin	Underground disclosures, wiki leaks, and sensitive information disclosure from various online attacks	http://pastebin.com/
Github	Source codes and other software centric information	http://www.github.com
Google Dorks Database	Database for finding exposed network devices and servers on the Internet	http://www.hackersforcharity.org/ghdb/ | http://www.exploit-db.com/google-dorks/
Google Blogosphere	Content (blog posts) released by the target	http://www.blogspot.com
Pentest Tools	Network information gathering tools repository	http://pentest-tools.com
iSeek	Target information by querying various resources and presenting in graph format	http://iseek.com/
Wigle	Information about WiFi networks	https://wigle.net/
Whois	Details about the registered domains and associated organizations	http://www.internic.net/whois.html

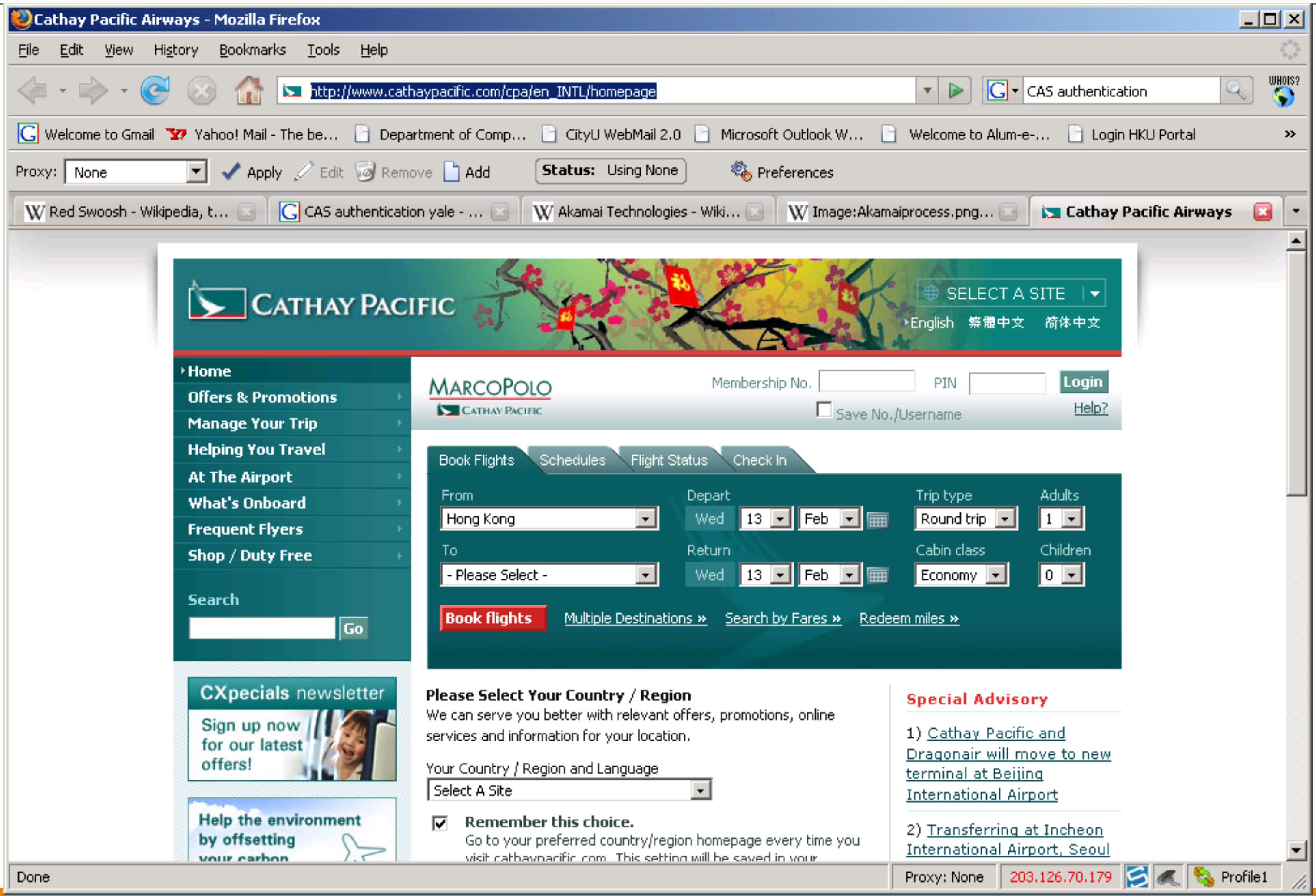
Intelligence Gathering Online Resources

Entity	Type of Information	Web Site
Institute of Electrical and Electronics Engineers (IEEE)	Information about research papers, journals, conferences proceedings, and associated people	http://www.ieee.org/index.html
Internet Assigned Numbers Authority (IANA)	Information about DNS root servers, IP address allocations, and Internet protocol resources	https://www.iana.org/

From: Targeted Cyber Attacks: Multi-Staged Attacks Driven by Exploits and Malware

Content Delivery Network

How come some servers response so fast



From	Depart	Trip type	Adults
Hong Kong	Wed 13 Feb	Round trip	1
To	**Return**	**Cabin class**	**Children**
- Please Select -	Wed 13 Feb	Economy	0

Please Select Your Country / Region

We can serve you better with relevant offers, promotions, online services and information for your location.

Your Country / Region and Language

Select A Site

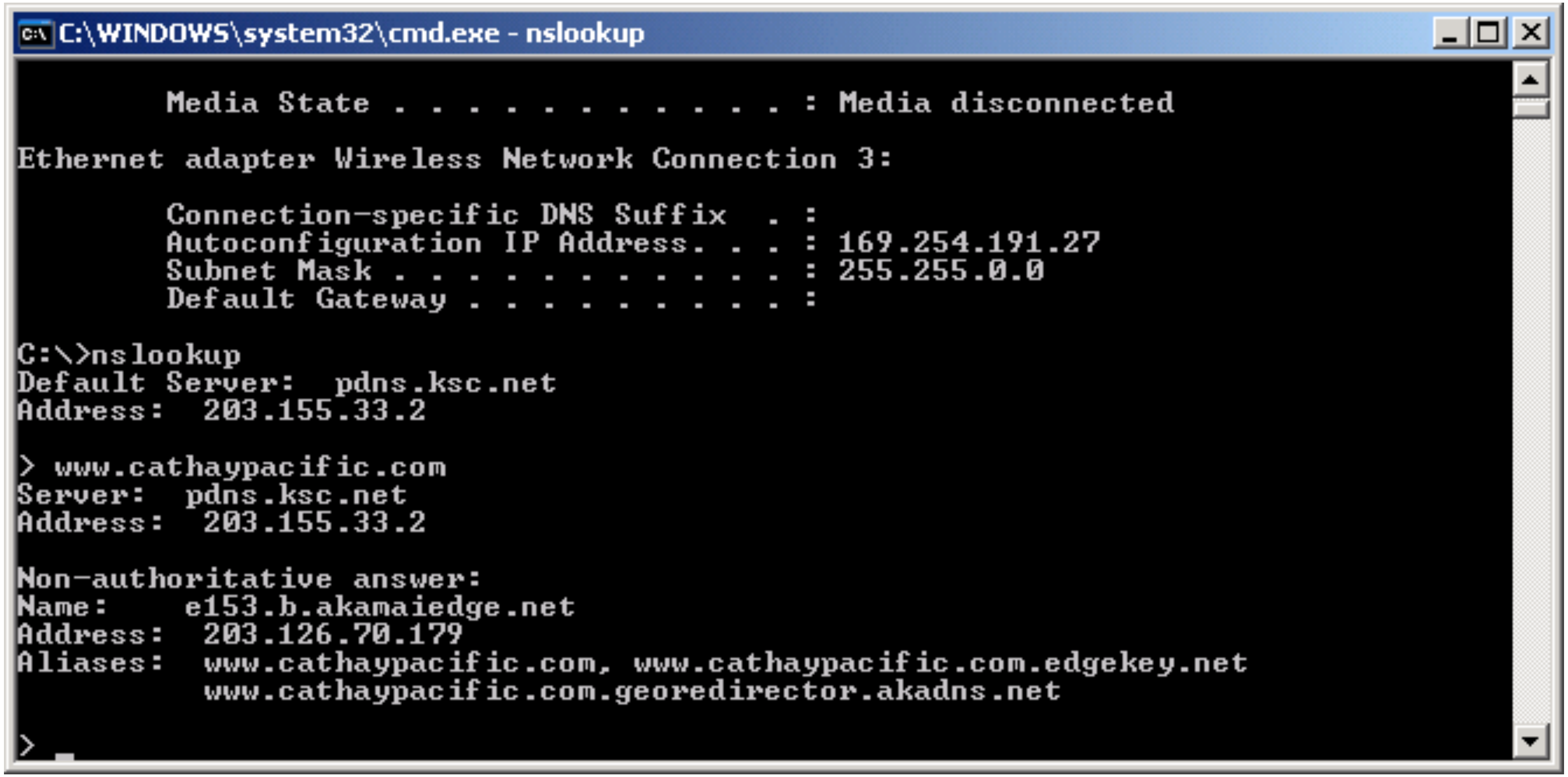
☑ **Remember this choice.**

Go to your preferred country/region homepage every time you visit cathaypacific.com. This setting will be saved in your

1) Cathay Pacific and Dragonair will move to new terminal at Beijing International Airport

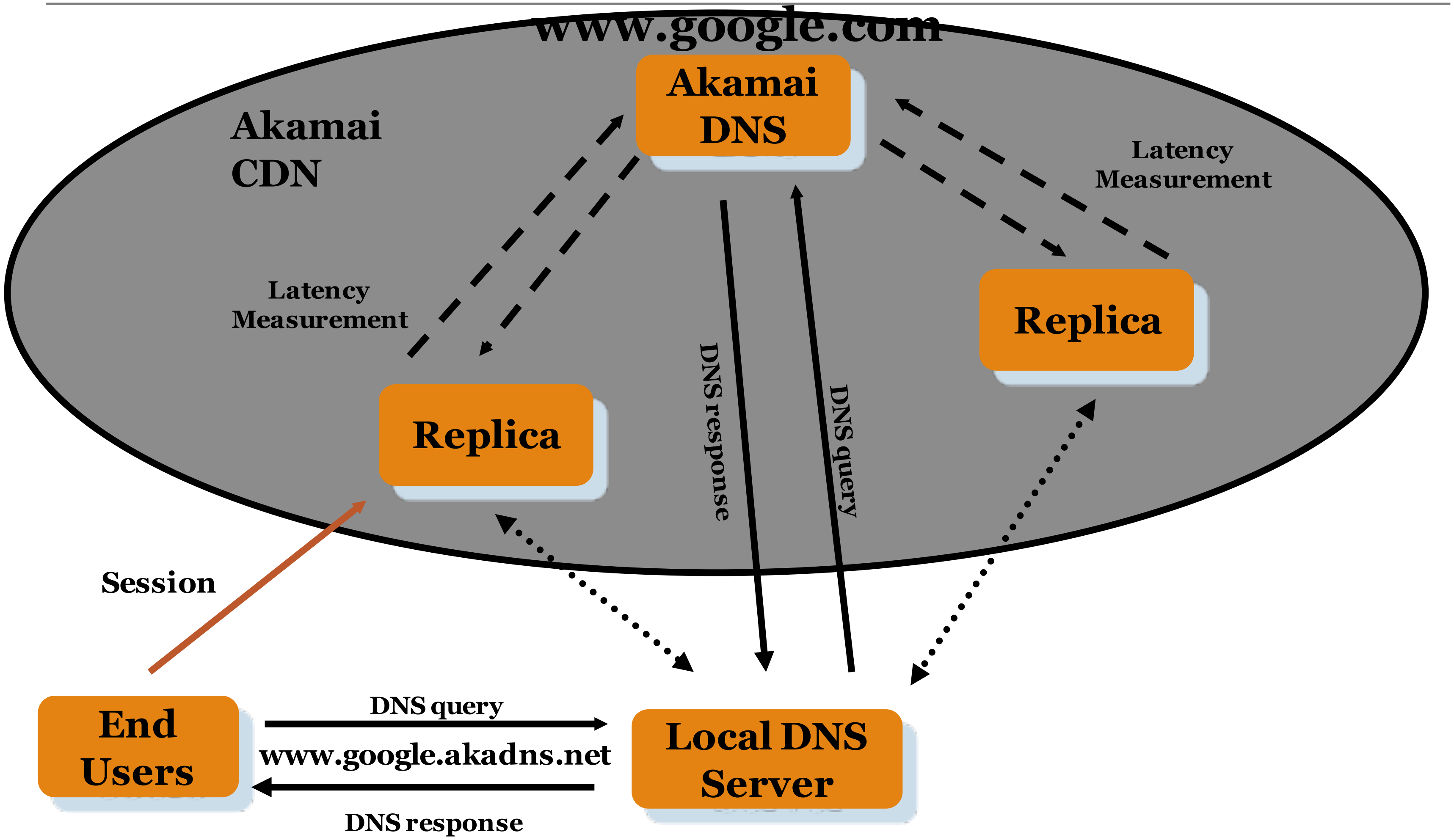
2) Transferring at Incheon International Airport, Seoul

The reason is Content Delivery Network (e.g. Akamai CDN)



```
        Media State . . . . . . . . . . . : Media disconnected

Ethernet adapter Wireless Network Connection 3:

        Connection-specific DNS Suffix  . :
        Autoconfiguration IP Address. . . : 169.254.191.27
        Subnet Mask . . . . . . . . . . . : 255.255.0.0
        Default Gateway . . . . . . . . . :

C:\>nslookup
Default Server:  pdns.ksc.net
Address:  203.155.33.2

> www.cathaypacific.com
Server:  pdns.ksc.net
Address:  203.155.33.2

Non-authoritative answer:
Name:    e153.b.akamaiedge.net
Address:  203.126.70.179
Aliases:  www.cathaypacific.com, www.cathaypacific.com.edgekey.net
          www.cathaypacific.com.georedirector.akadns.net

> _
```

DNS-based Request-Routing



How Akamai works

A combined technology on DNS and Cache server

Divert the traffic based on DNS from Akamai to Akamai cache server

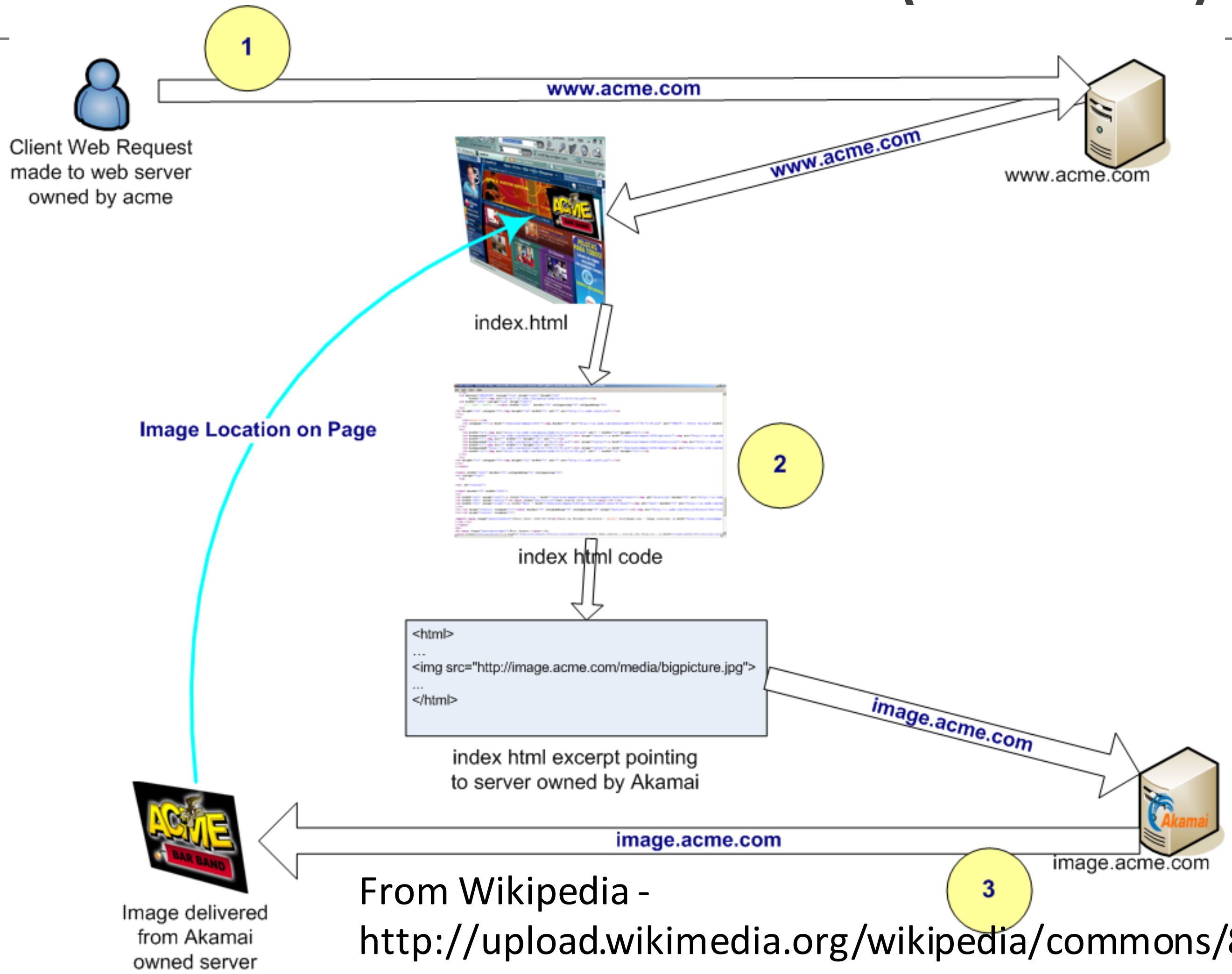
The Akamai DNS will provide the server information in a 20 seconds interview and each time 2 servers IP address will be provided

No server has to host all customer’s content for load balancing purpose

No customer is fully disconnected as there is another server

Content could be present at more than 2 servers at a site

How Akamai works (Cont.)



From Wikipedia - http://upload.wikimedia.org/wikipedia/commons/8/88/Akamaiprocess.pn

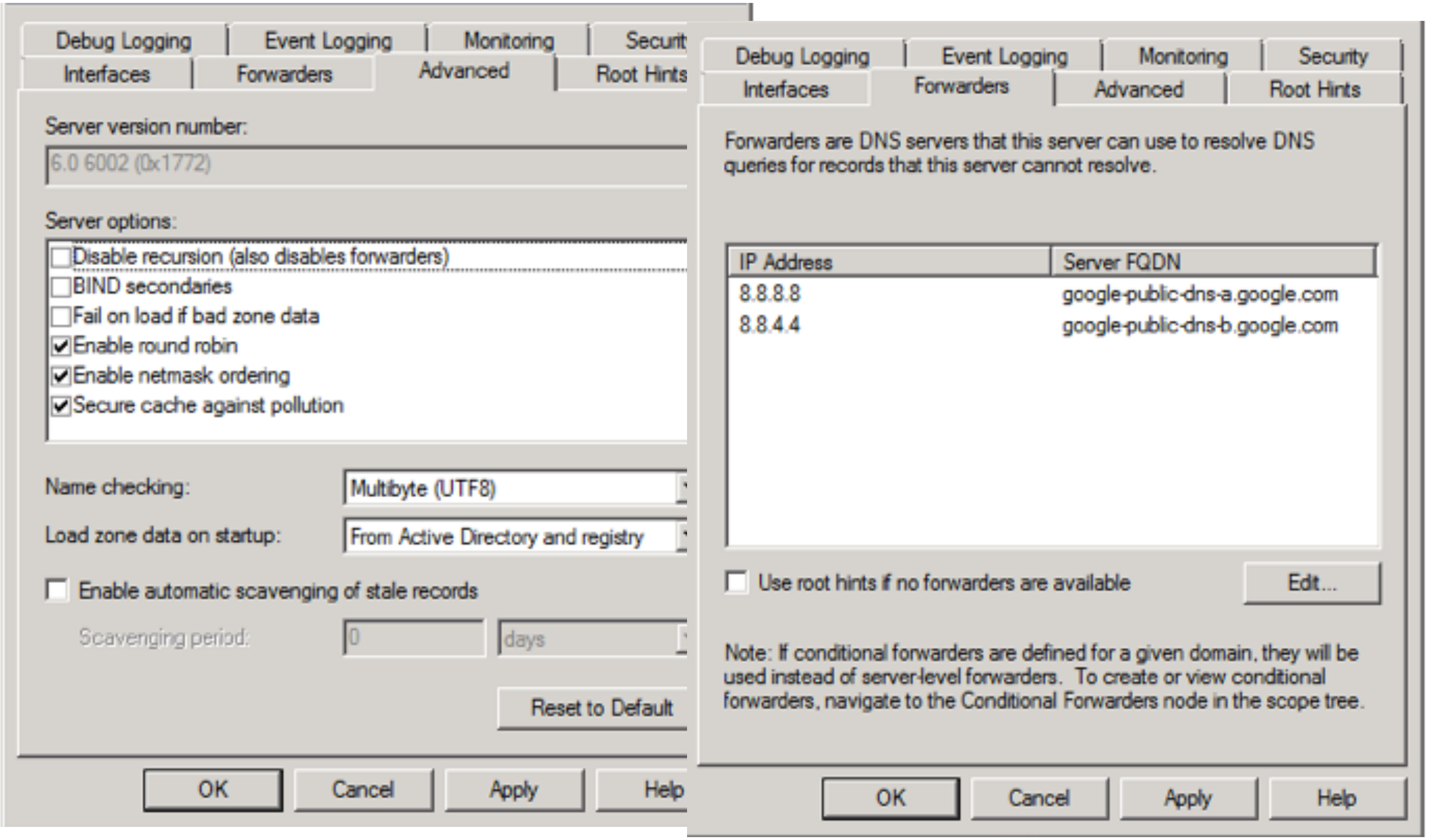
How Akamai works (Cont.)

Akamai provides services which

- accelerate dynamic and personalized content,
- J2EE-compliant applications, and
- streaming media to the extent that such services frame a localized perspective
- Through reverse proxy scheme to provide

DNS Security

DNS settings in Windows



Server version number:

6.0 6002 (0x1772)

Server options:

- □ Disable recursion (also disables forwarders)
- □ BIND secondaries
- □ Fail on load if bad zone data
- ☑ Enable round robin
- ☑ Enable netmask ordering
- ☑ Secure cache against pollution

Name checking: Multibyte (UTF8)

Load zone data on startup: From Active Directory and registry

□ Enable automatic scavenging of stale records

Scavenging period: 0 days

Forwarders are DNS servers that this server can use to resolve DNS queries for records that this server cannot resolve.

IP Address	Server FQDN
8.8.8.8	google-public-dns-a.google.com
8.8.4.4	google-public-dns-b.google.com

□ Use root hints if no forwarders are available

Note: If conditional forwarders are defined for a given domain, they will be used instead of server-level forwarders. To create or view conditional forwarders, navigate to the Conditional Forwarders node in the scope tree.

DNSSEC

The Domain Name System Security Extensions (DNSSEC) is a suite of Internet Engineering Task Force (IETF) specifications for securing certain kinds of information provided by the Domain Name System (DNS) as used on Internet Protocol (IP) networks.

It is a set of extensions to DNS which provide to

- DNS clients (resolvers) origin authentication of DNS data,
- authenticated denial of existence, and data integrity
- but not availability or confidentiality
- DNSSEC works by digitally signing records for DNS lookup using public-key cryptography.

DNSCurve

DNSCurve

- designed by Daniel J. Bernstein
- uses Curve25519 Elliptic curve cryptography (256-bit ECC) to establish keys used by Salsa20
- paired with the MAC function Poly1305
- used in CurveCP, a UDP-based protocol which is similar to TCP but uses elliptic-curve cryptography to encrypt and authenticate data
- to encrypt and authenticate DNS packets between resolvers and authoritative servers.
- Public keys for remote authoritative servers are placed in NS records, so recursive resolvers know whether the server supports DNSCurve

OpenDNS

OpenDNS offers DNS resolution as an alternative to using Internet service providers' DNS servers or locally installed DNS servers. OpenDNS has adopted and supports DNSCurve

IPv4

- 208.67.222.222
- 208.67.220.220

IPv6

- 2620:0:ccc::2
- 2620:0:ccd::2

Other DNS related functions

Phishing filter, OpenDNS also run a service called PhishTank for users to submit and review suspected phishing sites.

FamilyShield parental controls which block pornography, proxy servers, and phishing sites

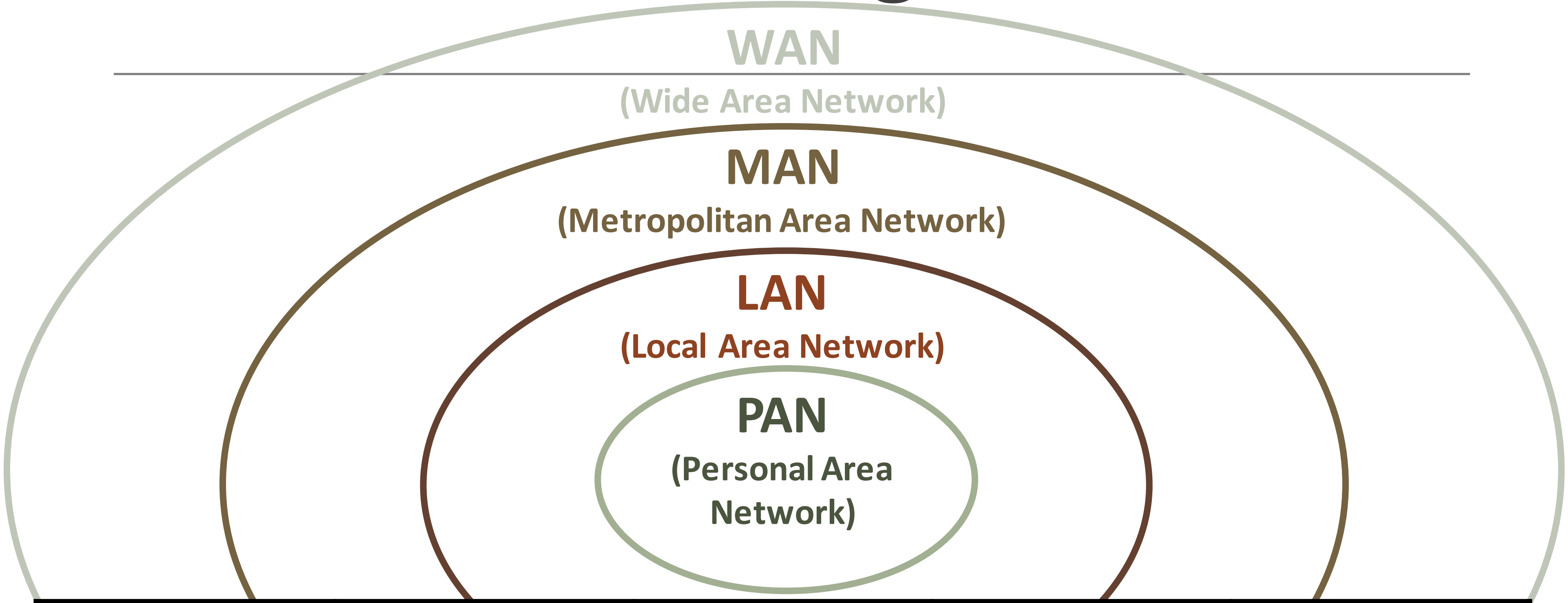
OpenDNS supports the DNSCrypt protocol, which authenticates DNS traffic between the user's computer and the name servers

OpenDNS Enterprise, a first foray into enterprise-grade network security.

OpenDNS Insights. This new service featured integration with Microsoft Active Directory, which allowed admins granular control over creating policies on a per-user, per-device, and per-group basis

WiFi Security

Wireless Technologies



WAN

(Wide Area Network)

MAN

(Metropolitan Area Network)

LAN

(Local Area Network)

PAN

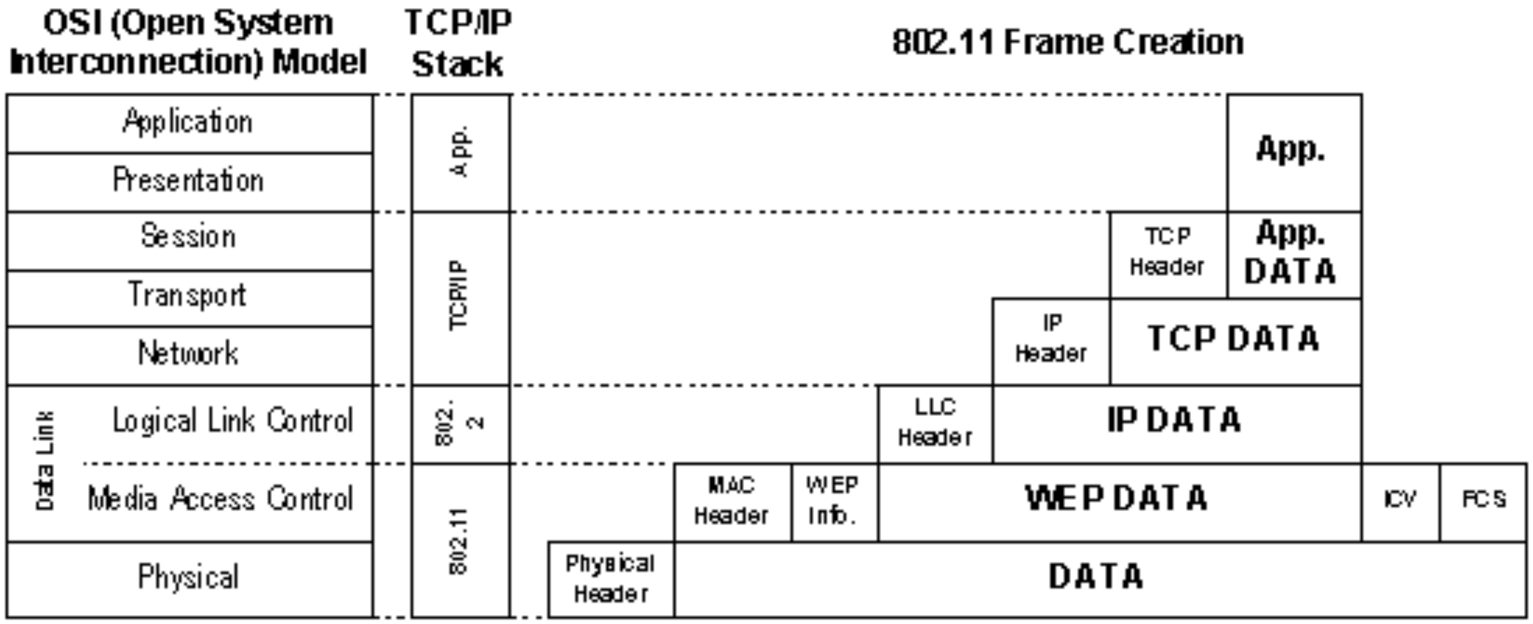
(Personal Area Network)

	PAN	LAN	MAN	WAN
Standards	Bluetooth	802.11 HiperLAN2	802.11 MMDS, LMDS, WiMAX	GSM, GPRS, CDMA, 2.5-3G
Speed	< 1Mbps	11 to 54 Mbps	11 to 100+ Mbps	10 to 384Kbps
Range	Short	Medium	Medium-Long	Long
Applications	Peer-to-Peer Device-to-Device	Enterprise networks	T1 replacement, last mile access	Mobile Phones, cellular data

WLAN IEEE 802.11 Standards

802.11a:	5GHz, 54Mbps
802.11b:	2.4GHz, 11Mbps
802.11c:	Wireless Bridging
802.11d:	Multiple regulatory domains
802.11e:	QoS and streaming extensions for 802.11a/g/h
802.11f:	Roaming for 802.11a/g/h Inter Access Point Protocol IAPP
802.11g:	54 Mbps WLAN in the 2.4 GHz band
802.11h:	Dynamic Frequency Selection (DFS) and Transmit Power Control (TPC)
802.11i:	Authentication and Encryption
802.11j:	Japan 802.11a additional Channels (4.9-5.1 GHz)
802.11k:	Exchange of capability information between client and access point
802.11m:	“Maintenance”, publication of standard updates
802.11n:	Next Generation WLAN with at least 100 Mbps

Network Layers in Wireless LAN



Basic Wi-Fi Network

Two basic components

- Access Points (AP) or Gateways.
  - Base stations - A bridge between wireless and wired networks
  - Wired network interface and Bridging software
  - Aggregates access for multiple wireless stations to wired network
- Radio
  - Aggregates access for multiple wireless stations to wired network. Wi-Fi radios
  - Embedded or attached to the PCs (e.g.: USB)
  - Notebooks embedded or with PCMCIA
  - Mobile devices

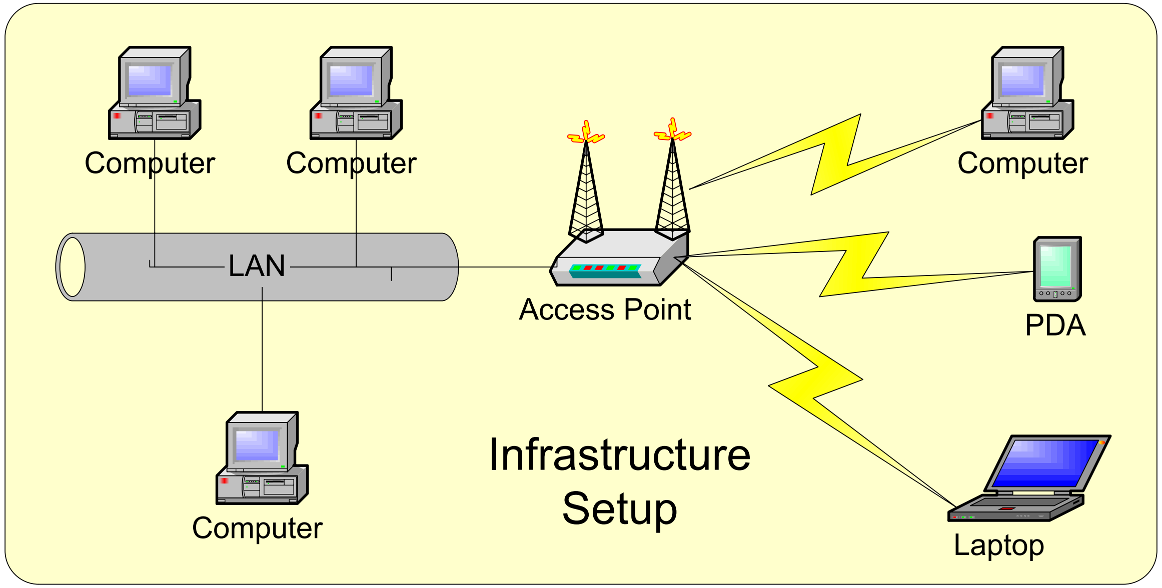
Infrastructure Mode

An access point (AP) is a shared device

Performance issues of shared hubs

Bridges allow for interconnection

Protocols/ applications work seamlessly



Wireless Security Focus Areas

Authenticity

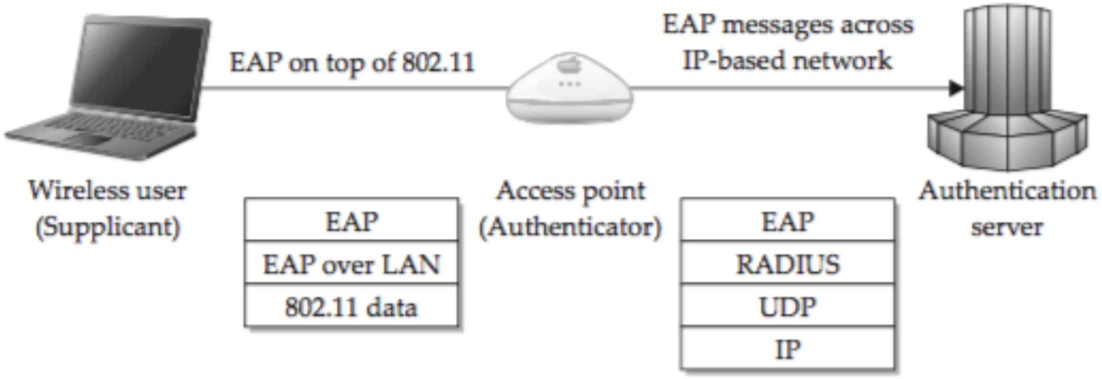
- Via BSSID (Basic Service Set ID), SSID, Wireless Encryption Scheme

Confidentiality

- Via encryption, Wireless Encryption Scheme

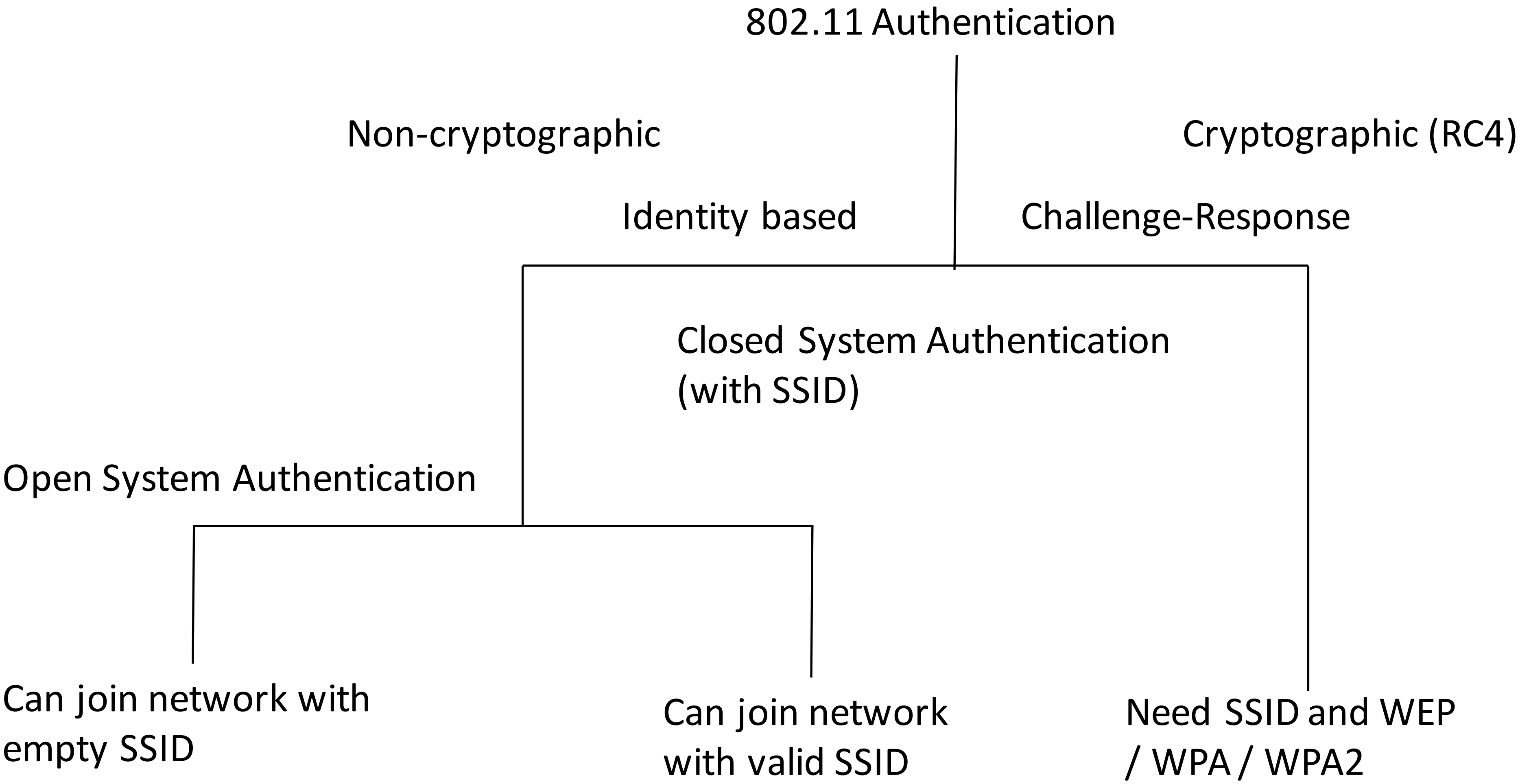
Integrity

- Via Wireless Encryption Scheme


EAP on top of 802.11
EAP messages across IP-based network
Wireless user (Supplicant)
Access point (Authenticator)
Authentication server
EAP
EAP over LAN
802.11 data
EAP
RADIUS
UDP
IP

From "Hacking Exposed Wireless 2nd Edition"

WLAN Authentication Concept



802.11 Authentication

Non-cryptographic

Cryptographic (RC4)

Identity based

Challenge-Response

Closed System Authentication
(with SSID)

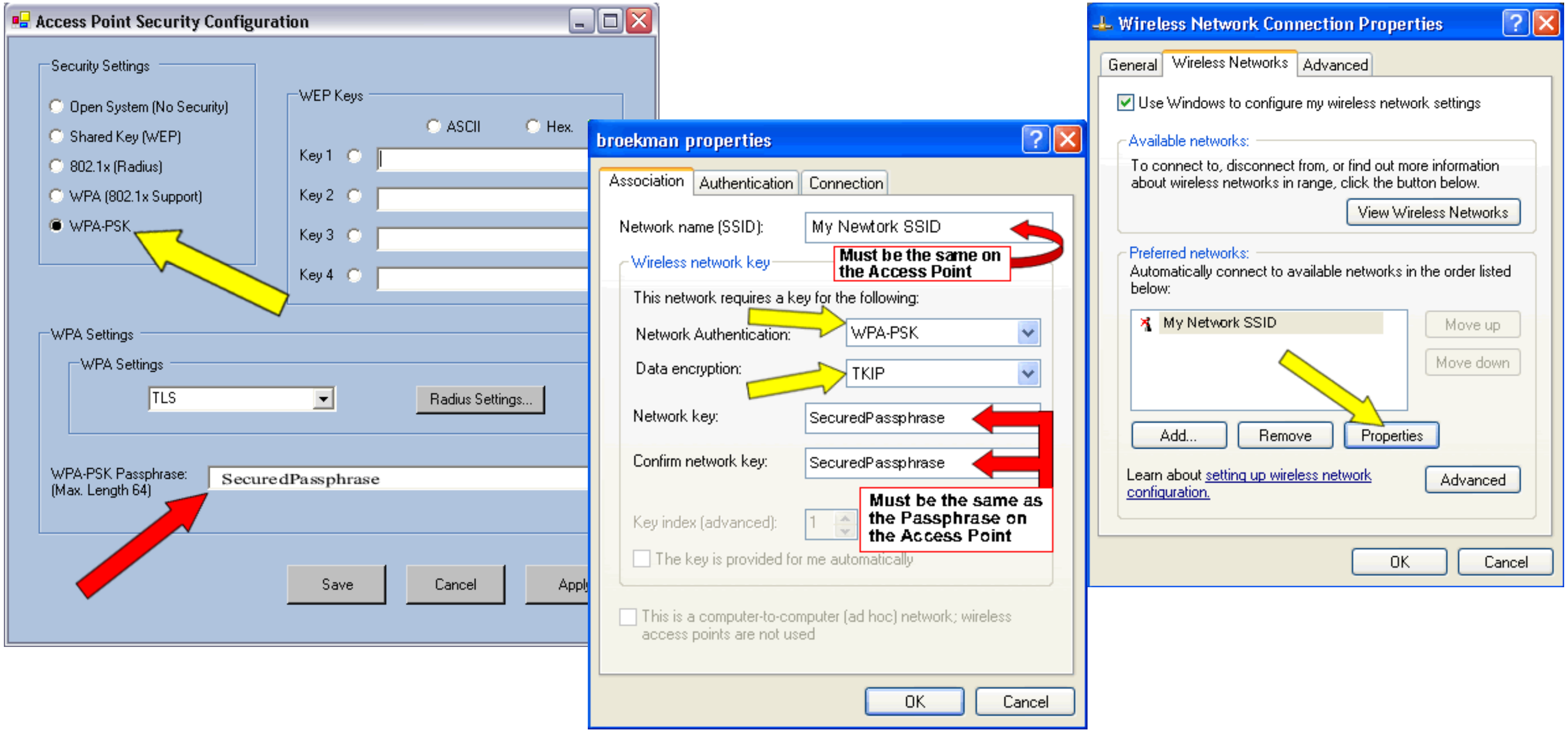
Open System Authentication

Can join network with
empty SSID

Can join network
with valid SSID

Need SSID and WEP
/ WPA / WPA2

WiFi settings



Access Point Security Configuration

Security Settings

○ Open System (No Security)
○ Shared Key (WEP)
○ 802.1x (Radius)
○ WPA (802.1x Support)
● WPA-PSK

WEP Keys: ○ ASCII ○ Hex.

Key 1 ○
Key 2 ○
Key 3 ○
Key 4 ○

WPA Settings

WPA Settings: TLS

WPA-PSK Passphrase: (Max. Length 64) SecuredPassphrase

broekman properties

Network name (SSID): My Newtork SSID

Must be the same on the Access Point

Wireless network key

This network requires a key for the following:

Network Authentication: WPA-PSK

Data encryption: TKIP

Network key: SecuredPassphrase

Confirm network key: SecuredPassphrase

Must be the same as the Passphrase on the Access Point

Key index (advanced): 1

□ The key is provided for me automatically

□ This is a computer-to-computer (ad hoc) network; wireless access points are not used

Wireless Network Connection Properties

☑ Use Windows to configure my wireless network settings

Available networks:

To connect to, disconnect from, or find out more information about wireless networks in range, click the button below.

Preferred networks:

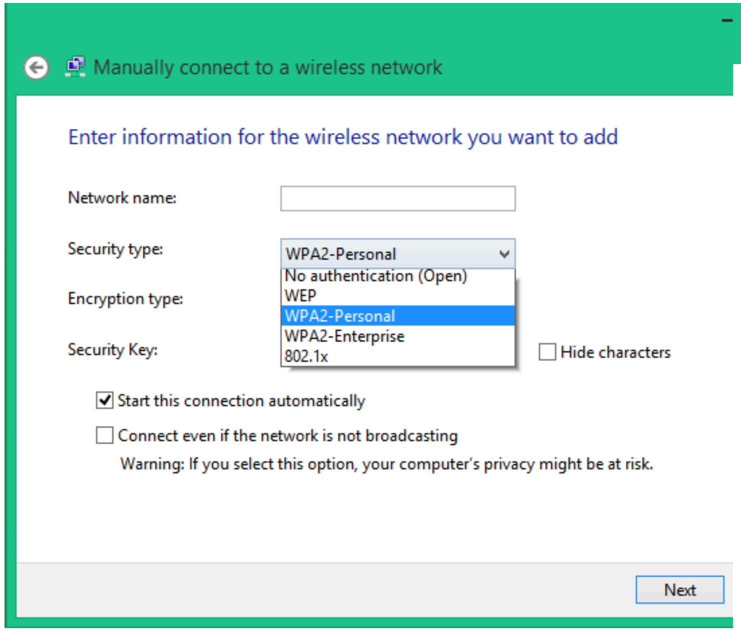
Automatically connect to available networks in the order listed below:

My Network SSID

Learn about setting up wireless network configuration.

http://www.wi-fiplanet.com

WiFi security related settings



Manually connect to a wireless network

Enter information for the wireless network you want to add

Network name:

Security type: WPA2-Personal

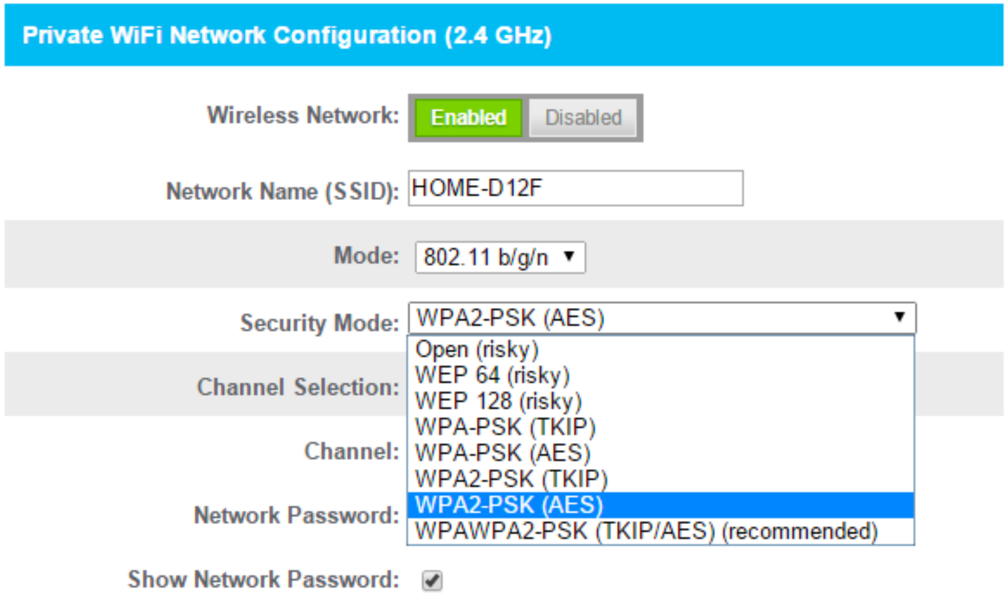
Encryption type:

Security Key: □ Hide characters

☑ Start this connection automatically

□ Connect even if the network is not broadcasting

Warning: If you select this option, your computer's privacy might be at risk.



Private WiFi Network Configuration (2.4 GHz)

Wireless Network: Enabled Disabled

Network Name (SSID): HOME-D12F

Mode: 802.11 b/g/n

Security Mode: WPA2-PSK (AES)

Channel Selection:

Channel:

Network Password:

Show Network Password: ☑

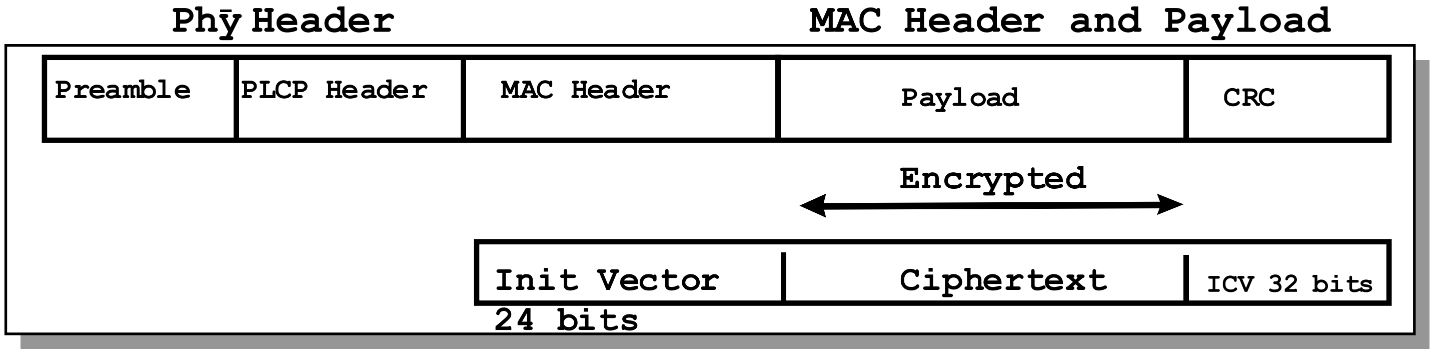
http://www.howtogeek.com/204697/wi-fi-security-should-you-use-wpa2-aes-wpa2-tkip-or-both/

Wired Equivalency Privacy

WEP: symmetric encryption (shared key), defines method but not how to share and distribute/manage keys

RC4 algorithm (40+24 bits keys) WIFI compliant

104 + 24 bits proprietary (non IEEE standards) but interoperable implementations (ie Lucent/Compaq - Cisco)



Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II WPA2

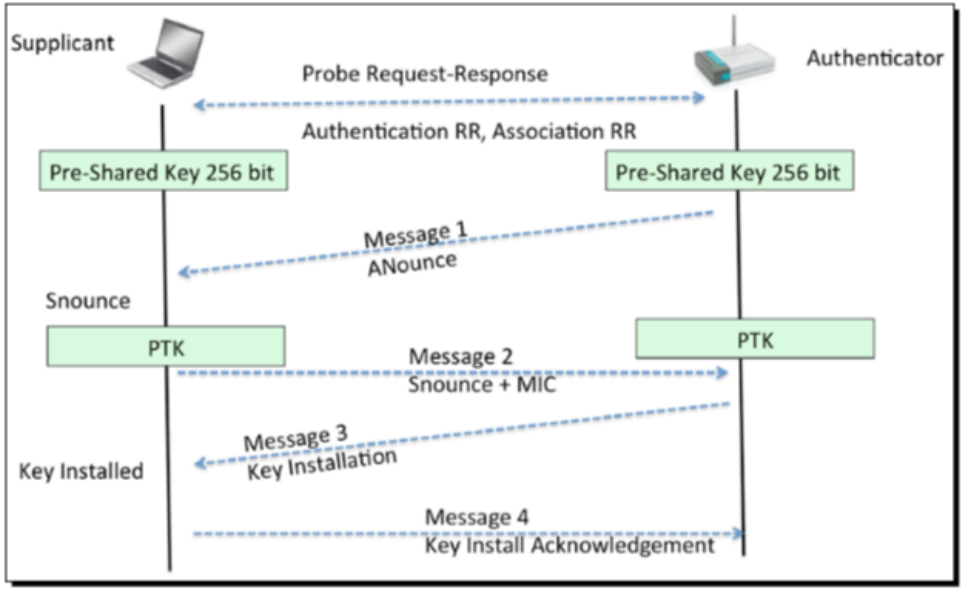
MODE	WPA	WPA2
ENTERPRISE MODE	Authentication: IEEE 802.1x EAP Encryption: TKIP/MIC (Mandatory) AES/CCMP	Authentication: IEEE 802.1x EAP Encryption: AES/CCMP
PERSONAL MODE	Authentication: PSK Encryption: TKIP/MIC	Authentication: PSK Encryption: TKIP/MIC

From “Kali Linux Wireless Penetration Testing” and
https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol
http://www.summitdata.com/blog/wpa2-enterprise-vs-wpa2-personal/

WPA and WPA 2 (Authentication Key Distribution)

Personal

- Pre-Shared Key authentication schema
  - This key may be entered either as a string of 64 hexadecimal digits, or as a passphrase of 8 to 63 printable ASCII characters

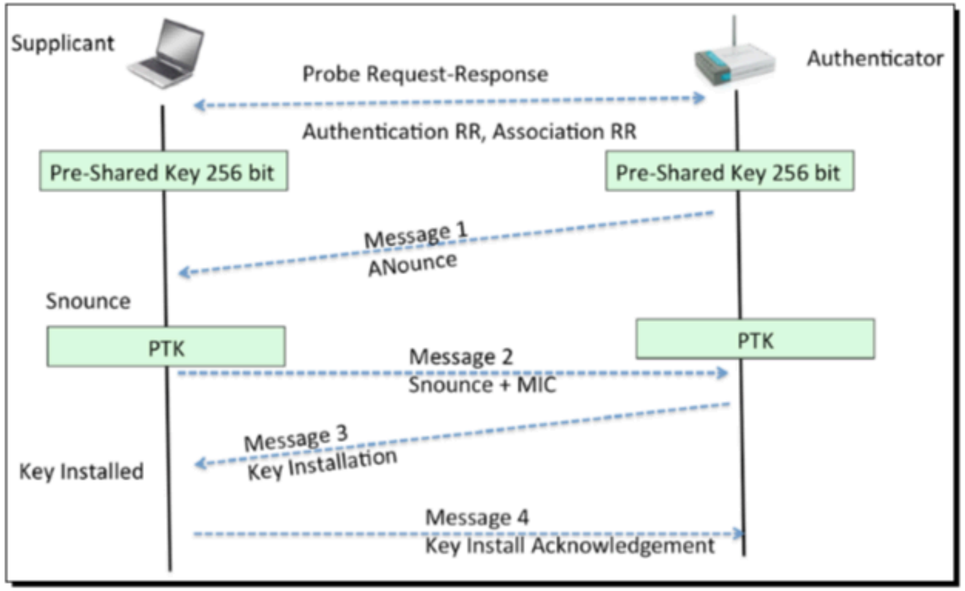


From Kali Wireless Penetration Testing, https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access

WPA and WPA 2 (Authentication Key Distribution)

Enterprise

- Referred as WPA-802.1X mode
  - designed for enterprise networks and requires a RADIUS authentication server.
- Support
  - EAP-TLS (previously tested)
  - EAP-TTLS/MSCHAPv2 (April 2005 [16])
  - PEAPv0/EAP-MSCHAPv2 (April 2005)
  - PEAPv1/EAP-GTC (April 2005)
  - PEAP-TLSEAP-SIM (April 2005)
  - EAP-AKA (April 2009 [17])
  - EAP-FAST (April 2009)



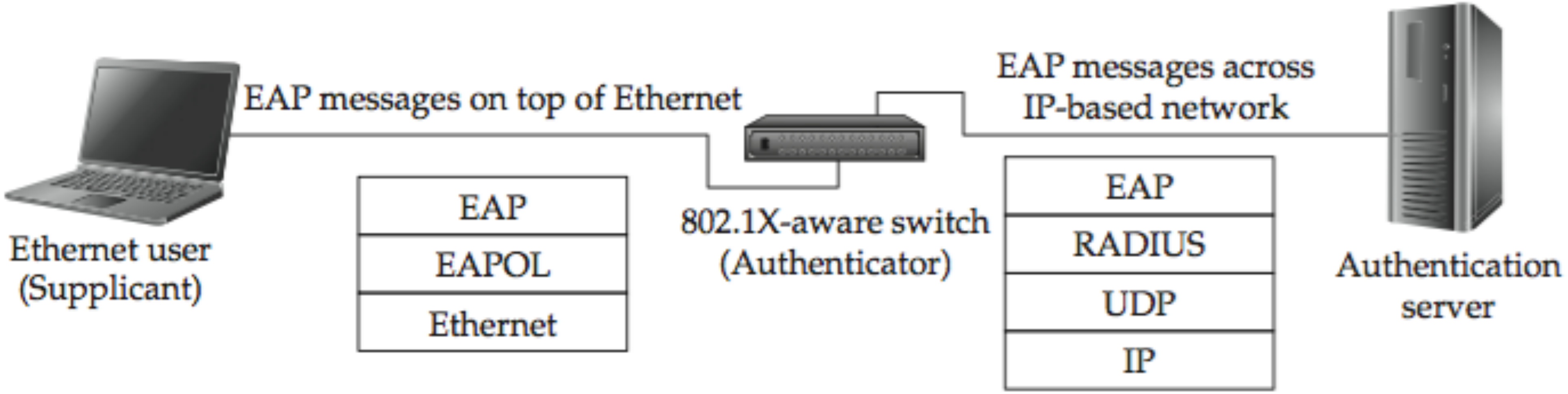
Includes Extensible Authentication Protocol (EAP) in April 2010 to WPA and WPA2

From Kali Wireless Penetration Testing, https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access

Extensible Authentication Protocol (EAP)

EAP is a very small protocol.

Fills up with layer two protocols such as Ethernet, layer three protocols such as IP, and so on.


EAP messages on top of Ethernet
EAP messages across IP-based network
Ethernet user (Supplicant)
802.1X-aware switch (Authenticator)
Authentication server

EAP
EAPOL
Ethernet

EAP
RADIUS
UDP
IP

WPA and WPA2 Encryption Scheme

Security protocols and security certification programs developed by the Wi-Fi Alliance to secure wireless computer networks

WPA

- Uses Temporal Key Integrity Protocol (TKIP) to replace 40/128 WEP encryption
  - 128-bit per-packet key
- Uses message integrity check

WPA2

- Replaces TKIP with Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP, AES-based encryption mechanism)
- Mandatory for devices bears the Wi-Fi trademark

Authentication key distribution

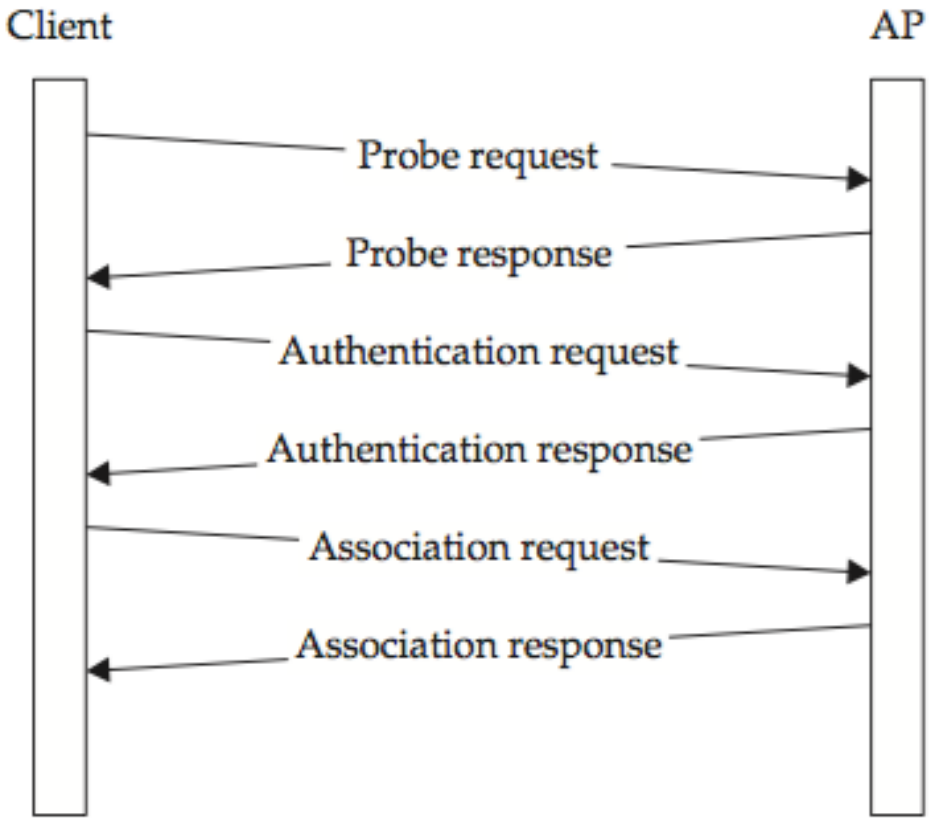
WPA-Personal

- Also referred to as WPA-PSK (Pre-shared key) mode.
- Designed for home and small office networks and doesn't require an authentication server
- Each wireless network device authenticates with the access point using the same 256-bit key

WPA-Enterprise

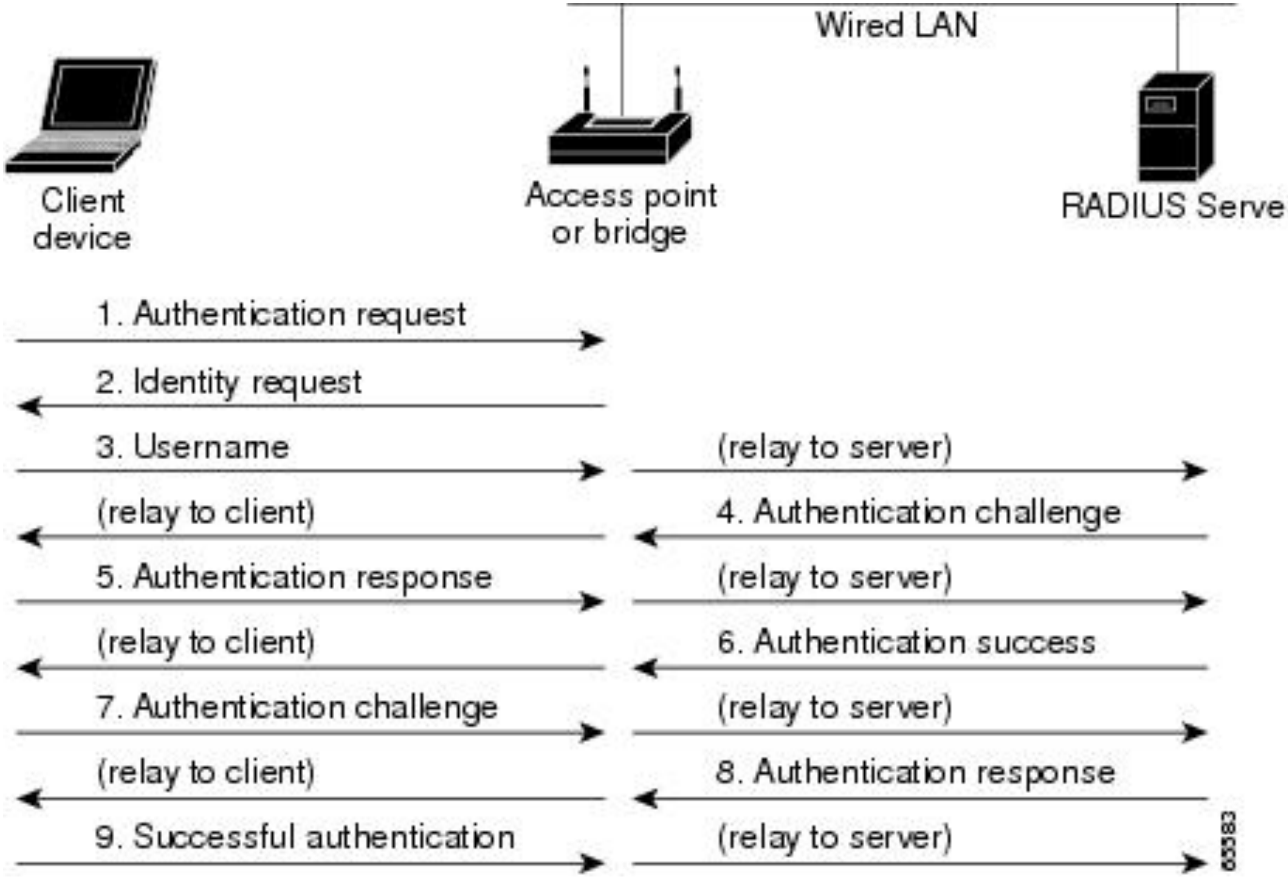
- Referred to as WPA-802.1x mode, and sometimes just WPA (as opposed to WPA-PSK)
- Designed for enterprise networks, and requires a RADIUS authentication server

Typical WiFi Authentication

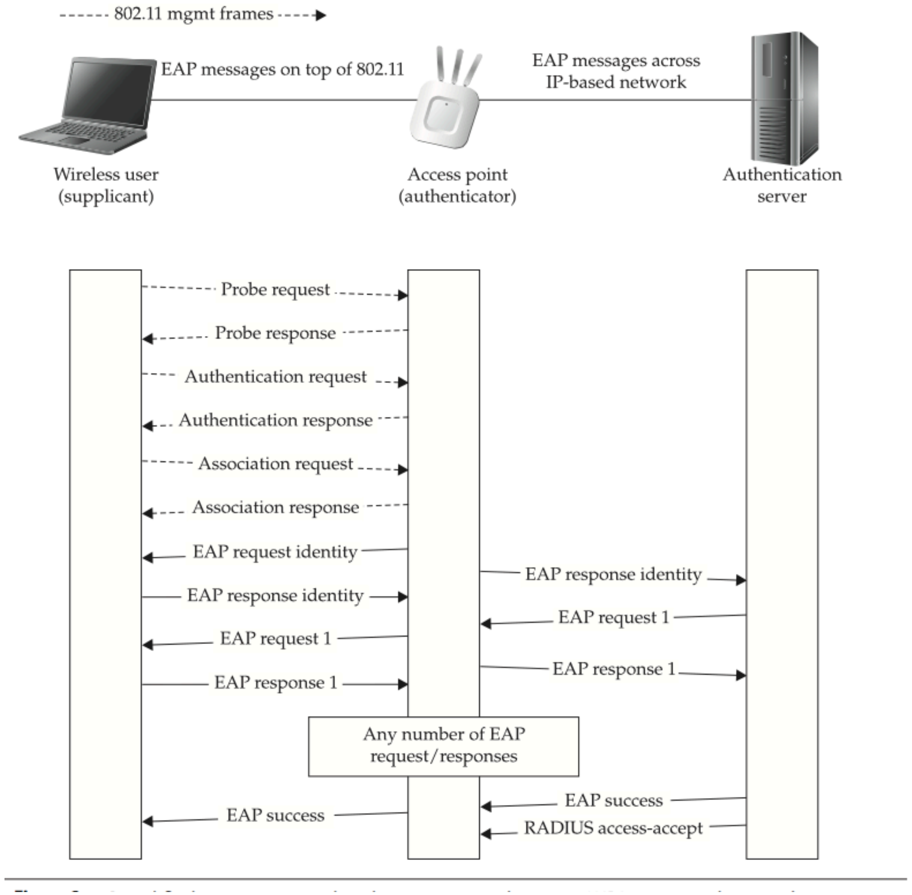


From: Hacking Exposed Wireless: Wireless Security Secrets & Solutions – Bonus Chapter

EAP Authentication to Network



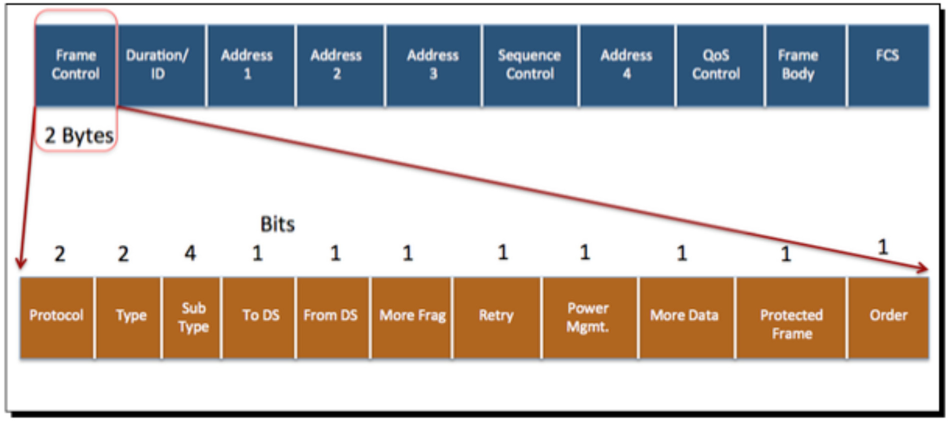
WPA Protocol



WLAN frames

Three types of WLAN frame

- Management frames are responsible for maintaining communication between AP and wireless clients
  - Authentication
  - Deauthentication
  - Association request
  - Association response
  - Reassociation request
  - Reassociation response
  - Disassociation
  - Beacon
  - Probe request
  - Probe response
- Control frames are responsible for ensuring a proper exchange of data between AP and wireless clients
  - Request to Send (RTS)
  - Clear to Send (CTS)
  - Acknowledgement (ACK)
- Data frames carry the actual data being sent to the wireless network



Frame Control	Duration/ ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	QoS Control	Frame Body	FCS

2	2	4	1	1	1	1	1	1	1	1
Protocol	Type	Sub Type	To DS	From DS	More Frag	Retry	Power Mgmt.	More Data	Protected Frame	Order

From Kali Wireless Penetration Testing

WLAN Management Frames

Authentication frame: 802.11 authentication is a process whereby the access point either accepts or rejects the identity of a radio NIC.

Deauthentication frame: A station sends a deauthentication frame to another station if it wishes to terminate secure communications.

Probe request frame: A station sends a probe request frame when it needs to obtain information from another station.

Probe response frame: A station will respond with a probe response frame, containing capability information, supported data rates, etc., when after it receives a probe request frame.

Beacon frame: The access point periodically sends a beacon frame to announce its presence and relay information, such as timestamp, SSID, and other parameters regarding the access point to radio NICs that are within range

How wireless network works?

Wireless network AP will broadcast or not broadcast their Service Set Identifier (SSID) depends on the configuration

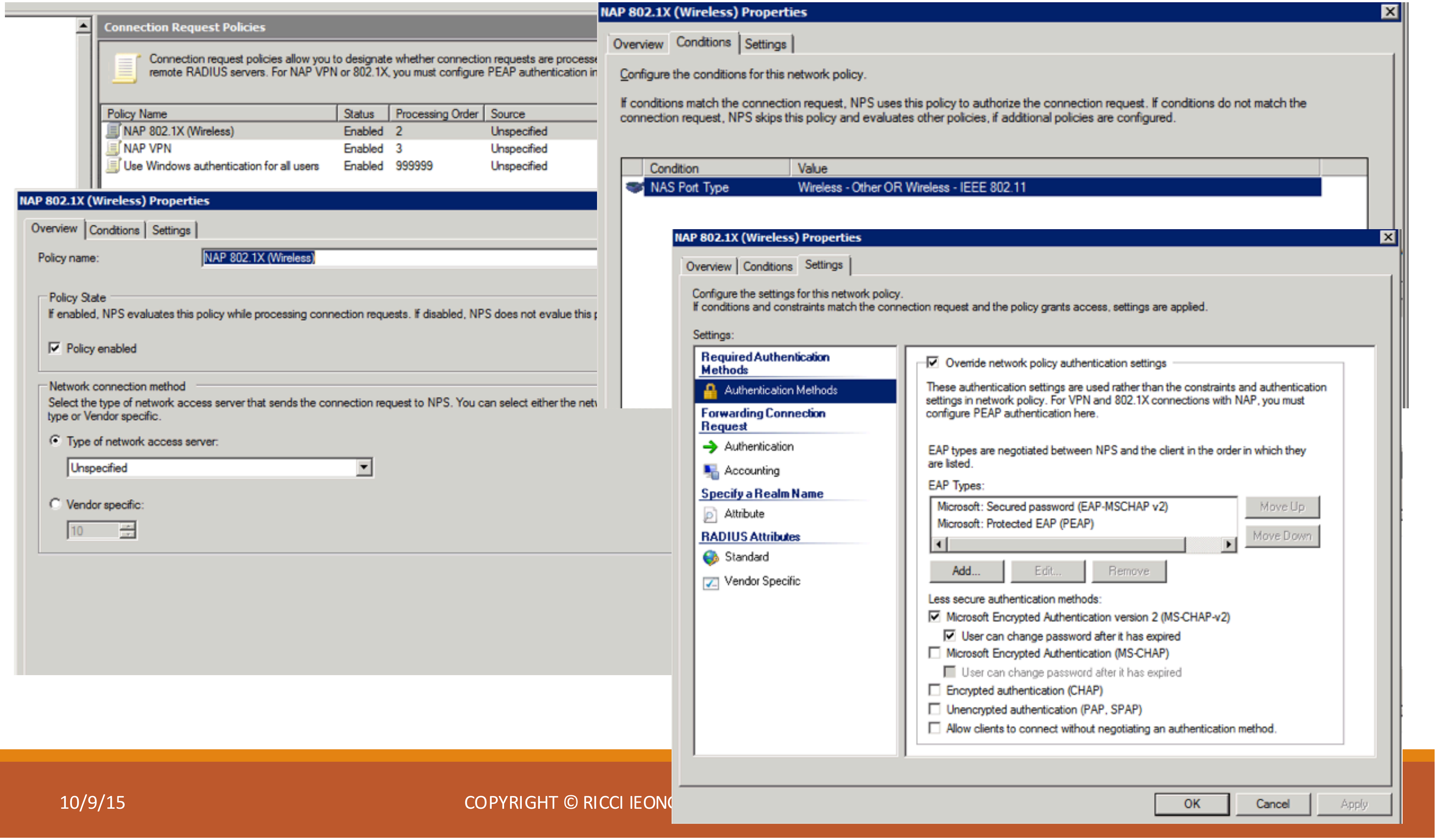
For Broadcast mode

- Beacon frames will be used to send SSID to the network

For non-broadcast mode

- Beacon frame will send NULL SSID value
- Client must search with probe requests where the probe frame contains SSID and will be sent out every 60 seconds

NAP 802.1 (Wireless) requirement



Connection Request Policies

Connection request policies allow you to designate whether connection requests are processe
remote RADIUS servers. For NAP VPN or 802.1X, you must configure PEAP authentication in

Policy Name	Status	Processing Order	Source
NAP 802.1X (Wireless)	Enabled	2	Unspecified
NAP VPN	Enabled	3	Unspecified
Use Windows authentication for all users	Enabled	999999	Unspecified

NAP 802.1X (Wireless) Properties

Overview | Conditions | Settings

Policy name: NAP 802.1X (Wireless)

Policy State

If enabled, NPS evaluates this policy while processing connection requests. If disabled, NPS does not evalue this p

☑ Policy enabled

Network connection method

Select the type of network access server that sends the connection request to NPS. You can select either the netw
type or Vendor specific.

● Type of network access server:

Unspecified

○ Vendor specific:

10

NAP 802.1X (Wireless) Properties

Overview | Conditions | Settings

Configure the conditions for this network policy.

If conditions match the connection request, NPS uses this policy to authorize the connection request. If conditions do not match the connection request, NPS skips this policy and evaluates other policies, if additional policies are configured.

Condition	Value
NAS Port Type	Wireless - Other OR Wireless - IEEE 802.11

NAP 802.1X (Wireless) Properties

Overview | Conditions | Settings

Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

Settings:

☑ Override network policy authentication settings

These authentication settings are used rather than the constraints and authentication settings in network policy. For VPN and 802.1X connections with NAP, you must configure PEAP authentication here.

EAP types are negotiated between NPS and the client in the order in which they are listed.

EAP Types:

Microsoft: Secured password (EAP-MSCHAP v2)
Microsoft: Protected EAP (PEAP)

Less secure authentication methods:

☑ Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)

☑ User can change password after it has expired

□ Microsoft Encrypted Authentication (MS-CHAP)

□ User can change password after it has expired

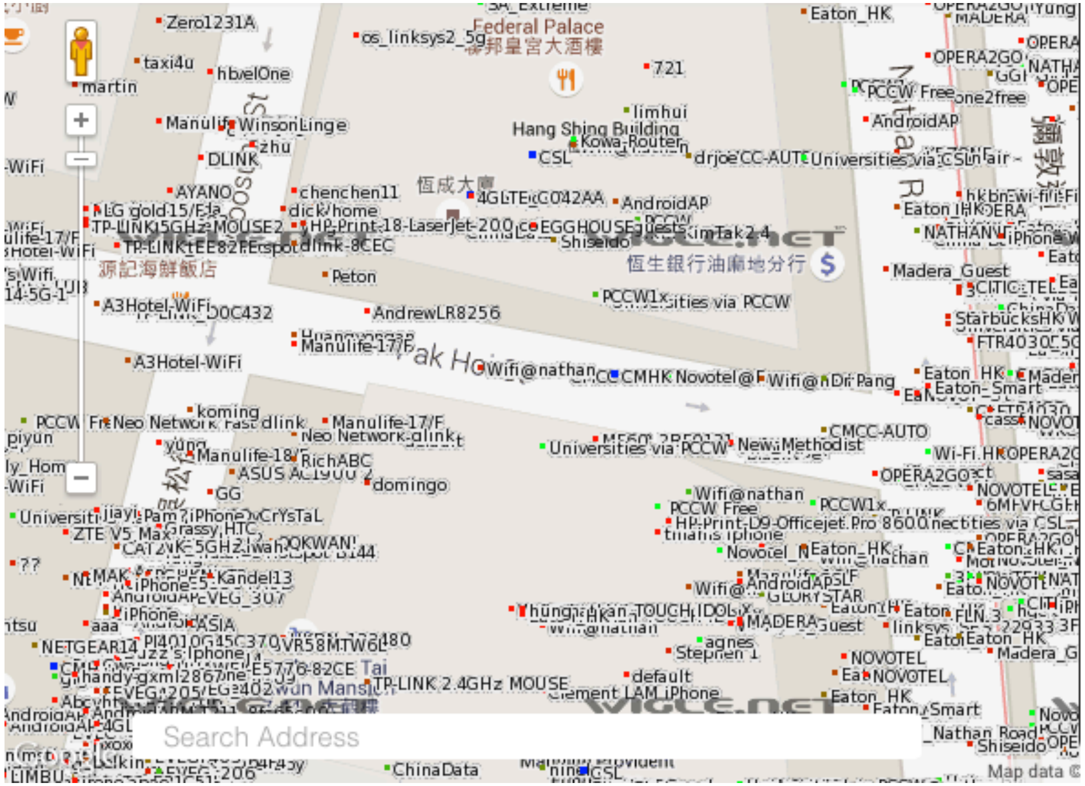
□ Encrypted authentication (CHAP)

□ Unencrypted authentication (PAP, SPAP)

□ Allow clients to connect without negotiating an authentication method.

Wireless LAN lab

http://wigle.net



Security Standards based on services

Area of application	Service	Security standard
Internet security	Network authentication	Kerberos
	Secure TCP/IP communications over the Internet	IPSec
	Privacy-enhanced electronic mail	S/MIME, PGP
	Public-key cryptography standards	3-DES, DSA, RSA, MD-5, SHA-1, PKCS
	Secure hypertext transfer protocol	S-HTTP
	Authentication of directory users	X.509/ISO/IEC 9594–8:2000:
	Security protocol for privacy on Internet/transport security	SSL, TLS, SET
Digital signature and encryption	Advanced encryption standard/PKI/ digital certificates, XML digital signatures	X509, RSA BSAFE SecurXML-C, DES, AES, DSS/DSA, EESSI, ISO 9xxx, ISO, SHA/ SHS, XML Digital Signatures (XMLD-SIG), XML Encryption (XMLENC), XML Key Management Specification (XKMS)
Login and authentication	Authentication of user’s right to use system or network resources	SAML, Liberty Alliance, FIPS 112
Firewall and system security	Security of local, wide, and metropolitan area networks	Secure Data Exchange (SDE) protocol for IEEE 802, ISO/IEC 10164

Joseph Migga Kizza (2015). Guide to Computer Network Security. Third Edition. Springer-Verlag London

Reference Books

Related content	Book	Chapter
W2 - LANs, WANs	Guide to Computer Network Security (2015)	Chapter 1: Computer Network Fundamentals
W2: Network Attack	Computer Security Principles and Practice (2012)	Chapter 8: Intrusion Detection
W2: WiFi Security	Computer Security Principles and Practice (2012)	Chapter 24: Wireless Network Security
W2: Wireless attack	Computer Security Handbook (2014)	Chapter 33: 802.11 Wireless LAN Security
W2: WiFi Security	Cryptography and Network Security (2011)	Chapter 17: Wireless Network Security