Understanding TCP/IP

Overview

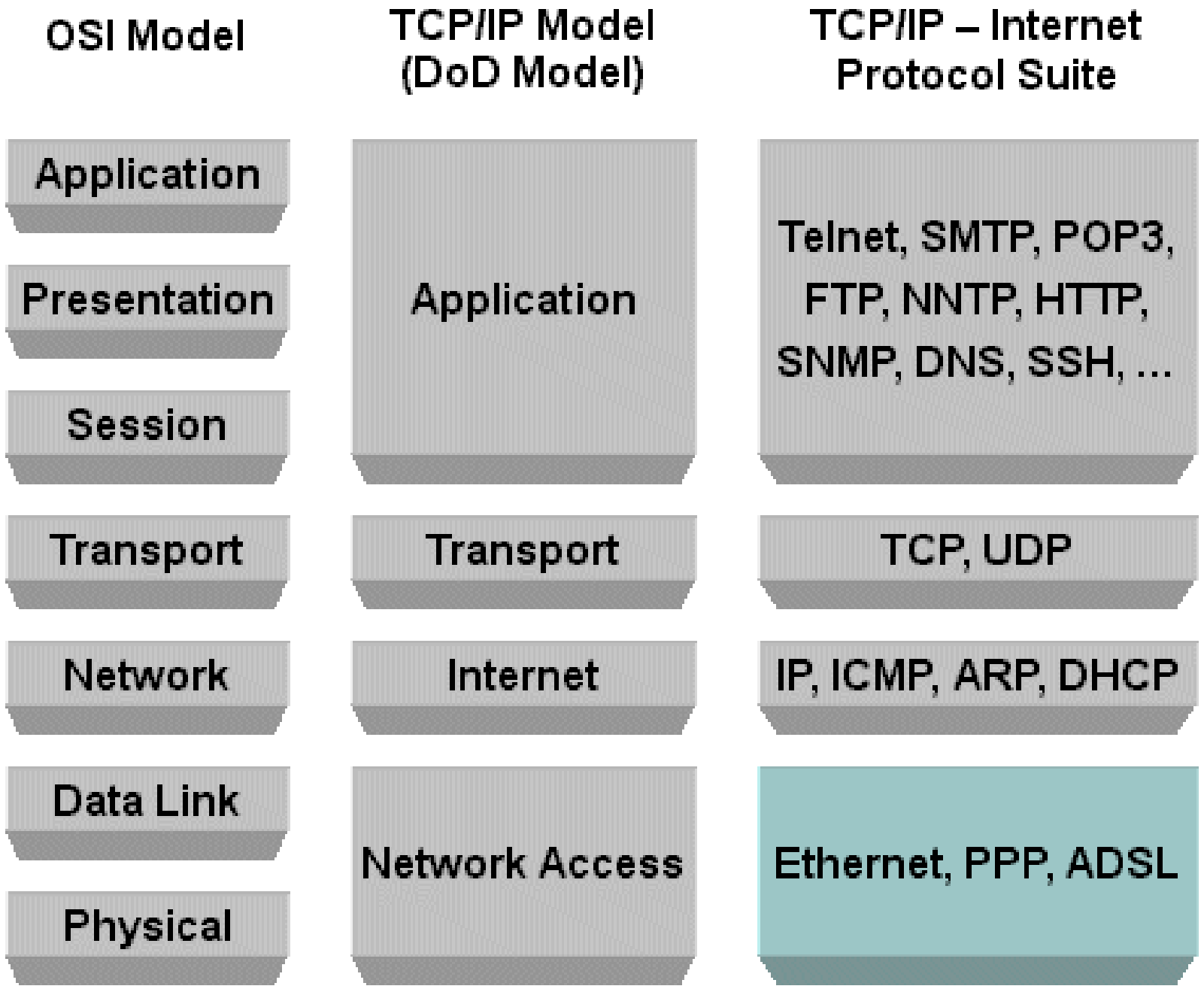
- Protocols are essential
- 1980s/1990s vendors designed their own
- TCP/IP – emerged as the dominant protocol
- 99% of networks (including Internet) use TCP/IP
- A foundation, not comprehensive

TCP/IP

- Transmission Control Protocol / Internet Protocol
- Non-proprietary (Nobody owns it)
- Routable (can switch to different networks)
- Underpins the internet
- Group of protocols
    - Addressing
    - Naming
    - Data delivery
-

Transmission Control Protocol/Internet Protocol

- Two Protocols
    - Transmission Control
    - Internet Protocol
- 100s of actual protocols implemented
- Implemented on many OS's
- TCP – Guaranteed information delivery
- Based on OSI 7 layer model
- DoD model maps 4 layers on OSI 7 layer model


OSI Model
TCP/IP Model (DoD Model)
TCP/IP – Internet Protocol Suite
Application
Presentation
Session
Application
Telnet, SMTP, POP3, FTP, NNTP, HTTP, SNMP, DNS, SSH, ...
Transport
Transport
TCP, UDP
Network
Internet
IP, ICMP, ARP, DHCP
Data Link
Physical
Network Access
Ethernet, PPP, ADSL

TCP/IP 4 Layers

- Most Protocols at the Process/Application Layer
  - HTTP – Hypertext Transfer Protocol
  - FTP – File Transfer Protocol
  - SMTP – Simple Mail Transfer Protocol
  - POP – Post Office Protocol
- Host to Host – 2 protocols
  - TCP – Transmission Control Protocol
  - UDP – User Datagram Protocol
- Internet – Backbone of the TCP/IP
  - ICMP – Internet Control Message Protocol
  - ARP – Address Resolution Protocol
- Network Layer – Describes the type of network access method

Process/Application Layer Protocols

- Layer provides differentiation and flexibility
- Need to know about the following for A+
- TFTP – Trivial File Transfer Protocol Protocol
    - Port 69
    - Light weight FTP
    - UDP (Conectionless)
    - 5 Commands
    - Mainly used for configuration transmission
- CIFS – Common Internet File System
    - MS enhancement of SMB
    - Port 445
    - Allows filesharing across OS's
    - Files and Printers
    - Default on Windows systems since Win 2000
- DHCP – Dynamc Host Configuration Protocol
    - Dynamic IP address and IP information
    - Reduces Administrator input
    - Ports 67, 68

Process/Application Layer Protocols Continued

- DNS – Domain Name System
  - Resolves URL (Uniform Resource Locator) to a physical IP Address
  - Port 53
- FTP – File Transfer Protocol
  - Copy, List, and Transfer of files.
  - Directory Management
  - Login required
  - Port 20/21
  - Also SFTP and FTPS
- HTTP – Hypertext Transfer Protocol
  - 1991
  - First effective Client-Server request-response protocol
  - Insecure - Plain text transmission
  - Port 80
- HTTPS – Hypertext Transfer Protocol Secure
  - 1994
  - Port 443
  - Security through (Encrypted Transmission)
    - SSL – Secure Sockets Layer (Certificates. Sometimes expire)
    - TLS – Transfer Layer Security

Process/Application Layer Protocols Continued

- IMAP – Internet Message Protocol
    - Email
    - Port 143
    - Replaces insecure POP3
    - Remains connected to server (Unlike POP3)
    - Stores emails on the server (Unlike POP3)
    - Allows multiple clients to a single mail box
        - Each client sees messages in real-time

Process/Application Layer Protocols Continued

- LDAP – Lightweight Directory Access Protocol
    - Based on X.500 standard
    - Allows access to information stored in an information directory
        - LDAP directory
        - LDAP database
    - Uses ACL (Access Control Lists) for permissions
    - Port 389

Process/Application Layer Protocols Continued

- NetBIOS/NetBT
  - Network Basic Input/Output System
  - API (Application Programming Interface) that allows computers to communicate across the network.
  - Layer 5 of the OSI model.
    - NetBIOS running over TCP/IP is called NetBT
  - Naming service (name registration and resolution)
  - Datagram distribution service (for connectionless)
  - Session management service (for connection orientated)
  - MS network clients had a NetBIOS name that was the network name
    - Names were resolved with an IP address with a WINS (windows internet name service)
    - Eventually they used DNS
  - Port 137/139

Process/Application Layer Protocols Continued

- POP3 – Post Office Protocol
  - Original protocol for email systems
  - Replaced by IMAP4
  - Port 110
- SFTP – Secure File Transfer Protocol
  - Secure alternative to FTP
- SMB – Server Message Block / CIFS – Common Internet File System
  - IBM development enhanced by Microsoft (and other vendors)
  - Shares files, printers and network resources
  - Similar to FTP but more options
  - Port 445
  - CIFS – Developed by MS to share files and printers

Process/Application Layer Protocols Continued

- RDP – Remote Desktop Protocol
  - Microsoft developed
  - Connection to remote computers
  - As if you were sitting at the PC
  - All keyboard and mouse commands encrypted
  - Supports sound, drive, port and network printer redirection
  - Remote workers and Technical Support
  - Port 3389
- SMTP – Simple Mail Transfer Protocol
  - Commonly used to send email messages
  - Push protocol
  - Server to Server communication as well as Server to Client
  - Port 25

Process/Application Layer Protocols Continued

- SNMP – Simple Network Management Protocol
    - Gathers and manages Network performance information
    - Port 161, 162
    - SNMP Server - Management device
        - Collects data from routers/switches
- SSH – Secure Shell
    - Used by Telnet
    - Remote PC Login
    - Common client OpenSSH
    - Port 22
- Telnet
    - Terminal emulation protocol
    - Remote Login to computers
    - Text only
    - Insecure - Plain text
    - Port 23

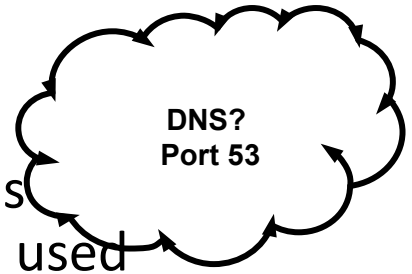
Host To Host (Transport) Layer Protocols

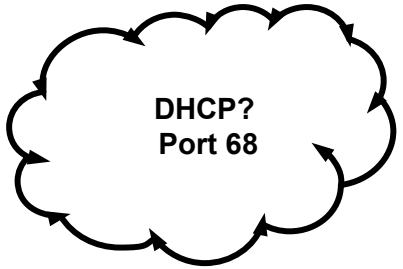
- UDP – User Datagram Protocol
  - Connectionless
  - Faster
  - Best Effort (no flow control)
  - VOIP, Streaming Music
- TCP – Transmission Control Protocol
  - Connection Orientated
  - Slower
  - Guarantee (Reassemble and resending)
    Email, Web Browsing

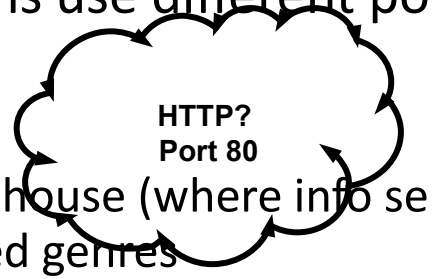
TCP	UDP
Reliable	Unreliable
Connection-oriented	Connectionless
Segment retransmission and flow control through windowing	No windowing or retransmission
Segment sequencing	No sequencing
Acknowledge segments	No acknowledgement

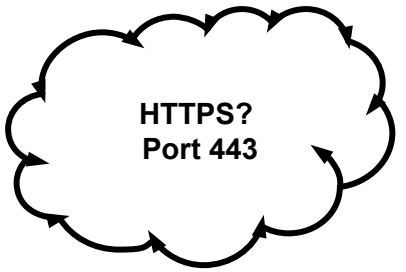
TCP and UDP

- Port Numbers
  - Keeps track of connections
  - Ensure right protocols are used
  - Differing applications use different ports
  -
  - Think of Cable TV
    - IP Address is house (where info sent)
    - Channels fixed genres
  - Or Imagine Block of flats mail room
  -
  - 65536 ports per IP Address
    - 0 to 1023 – Well known Ports
    - 1024 to 49151 – Registered Ports
    - 49152 to 65535 – Vendor Ports
  -
  -









Service	Protocol	Port(s)
FTP	TCP	20,21
SSH	TCP	22
Telnet	TCP	23
SMTP	TCP	25
DNS	TCP/UDP	53
DHCP	UDP	67,68
TFTP	UDP	69
HTTP	TCP	80
POP3	TCP	110
NetBIOS/NetBT	TCP	137,139
IMAP4	TCP	143
SNMP	UDP	161,162
LDAP	TCP	389
HTTPS	TCP	443
SMB/CIFS	TCP	445
RDP	TCP	3389

Internet Layer Protocols

- IP – Internet Protocol
- Manages logical network addresses
- Gets data from one place to another (even if there are many hops)
- Three Support protocols
    - ICMP – Delivers Error messages
        - Ping uses ICMP
    - ARP – resolves logical IP addresses to physical MAC addresses
    - RARP – Reverse ARP – resolves MAC addresses to IP addresses

IP Addressing

- IPv4 and IPv6
- Each device must have a unique address
- IPv4 – 32 bit hierarchical address
    - Example - 192.168.10.55
    - Each number is 8 bits (1 byte)
    - Each number called Octet
    - Above address in Binary as PC sees it:
      11000000 10101000 00001010 00110111

IPv4 Addressing

Network segment

Node segment

Binary **11010000.01111011.00101101.00010010**

Decimal **208.123.45.18**

Binary

	Octet - 1	Octet - 2	Octet - 3	Octet - 4
In Binary	11000000	10101000	00001010	00000001
	8 bits	8 bits	8 bits	8 bits
In Decimal	192	168	10	1

Total 32 bits

Binary Continued

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1
1	1	0	0	0	0	0	0

= 192

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1
1	0	1	0	1	0	0	0

= 168

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1
0	0	0	0	1	0	1	0

= 10

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1
0	0	0	0	0	0	0	1

= 1

IP Address Parts

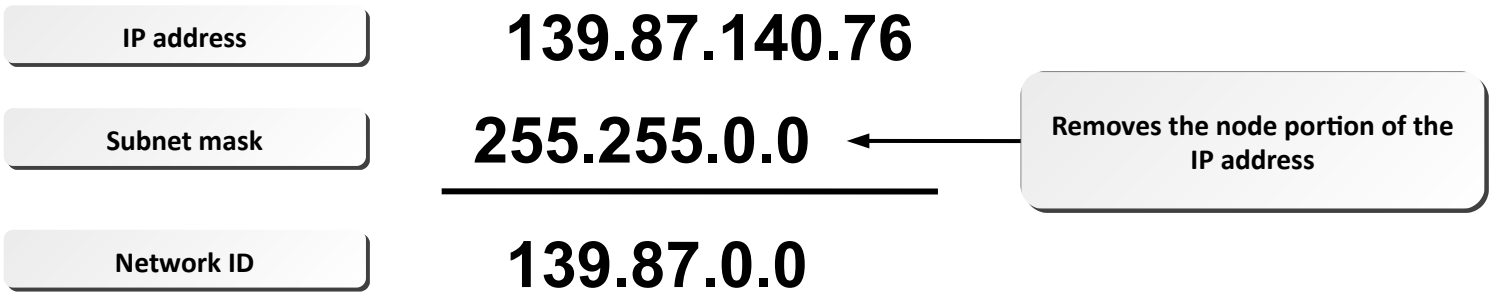
- All Ip addresses have a:
  - Network ID
  - Host ID
- Network comes before Host
  - No specified length for Network ID
  - In Octets but only 32 bits in total
- All addresses must be unique
- Network and host cannot be all 0s
  - Host ID portion of 0 means this network
- Network and host cannot be all 1s
  - Host ID portion of 1 means “all hosts on this network” – broadcast address

Subnet Mask

- Same format as IP an IP address
- Defines where network ID ends and Host address begins
- Anything marked as 255 defines the Network ID
- Anything else defines the Host ID

Subnet Mask 255.255.255.0				
	24 bits for Network ID			8 bits for Host ID
Decimal	255	255	255	0
Binary	11111111	11111111	11111111	00000000

Subnet Masks



Subnet Mask Continued

Subnet Mask 255.255.255.0				
	24 bits for Network ID			8 Bits for Host ID
Decimal	255	255	255	0
Binary	11111111	11111111	11111111	00000000

IP Address 192.168.10.55				
Decimal	192	168	10	55
Binary	11000000	10101000	00001010	00110111

IPv4 Address Classes

- Classes designated on first Octet
-

Class	Range	Subnet Mask	Comments
A	0 to 127	255.0.0.0	Very Large Networks First 8 Bits Network ID, remaining 24 bits Host ID 126 Network A addresses available – none available Telecom giants and very large global companies
B	128 to 191	255.255.0.0	Medium Sized Networks First 16 Bits Network ID, remaining 16bits Host ID (2^{14})16384 Networks with up to (2^{16}-2) 65534 hosts on each network Microsoft, Exxon Mobile etc
C	192 to 223	255.255.255.0	Smaller Networks First 24 Bits Network ID, remaining 8 bits Host ID (2^{21})2097152 networks with up to (2^{8}-2) 254 hosts on each network. Most companies use class C.
D	224 to 239	N/A	Reserved for multicasts (sending messages to multiple systems)
E	240 to 255	N/A	Reserved for testing

IPv4 Address Classes

- MIT has Class A network 18.0.0.0
- Nobody else can use 18.0.0.0
- Internal company networks can use this range as addresses will get translated at router

Class Examples

Class C - Example 192.168.1.x	Class B - Example 172.16.x.x	Class A – Example 10.x.x.x
192 168 1 1 N N N H 192 168 1 2 192 168 1 3 192 168 1 4 . . . 192 168 1 255	172 16 0 1 N N H H	10 0 0 1 N H H H

Further Class Maths (For Information only)

Network

Class - A	8 network bits	2^{8}	=	256
Class - B	16 network bits	2^{16}	=	65536
Class - C	24 network bits	2^{24}	=	16777216

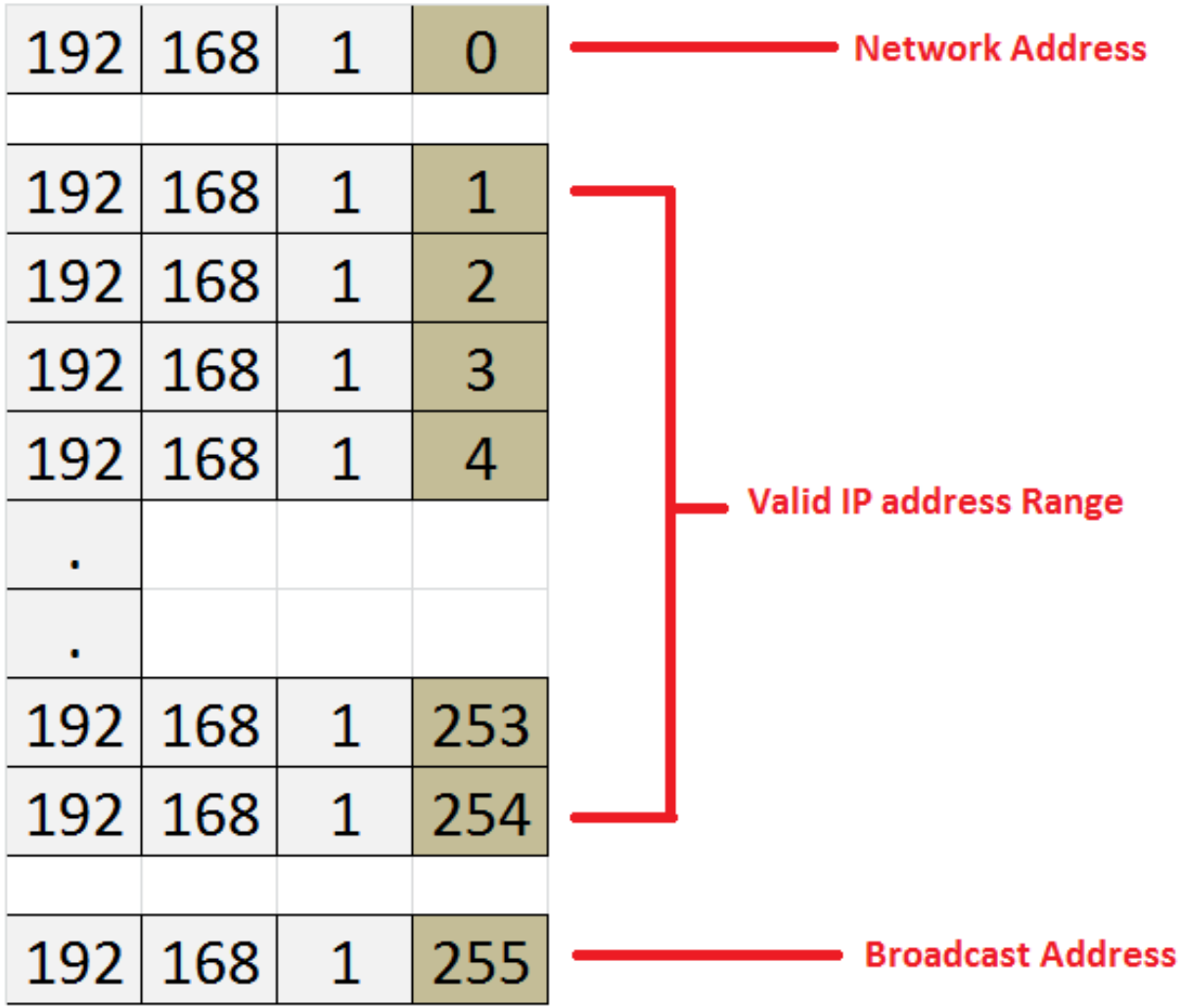
Host

Class - A	24 host bits	2^{24}	=	16777216
Class - B	16 host bits	2^{16}	=	65536
Class - C	8 host bits	2^{8}	=	256

We cannot have the values of all 0s or all 1s so need to subtract 2 from the totals

Class - A	24 host bits	2^{24}	=	16777216 - 2
Class - B	16 host bits	2^{16}	=	65536 - 2
Class - C	8 host bits	2^{8}	=	256 – 2

Class C valid IP address example



Classes Default Subnet Masks

Class - A	N. H. H. H	255.0.0.0
Class - B	N. N. H. H	255.255.0.0
Class - C	N. N. N. H	255.255.255.0

- IP addresses in range 127.x.x.x are only for testing
- IP address can be written in shorthand indicating the network portion of the address.
  - 10.0.0.0/8 indicates first 8 bits are network ID and remaining 24 bits Host ID
  - 192.168.1.0/24 – Class C with default subnet mask

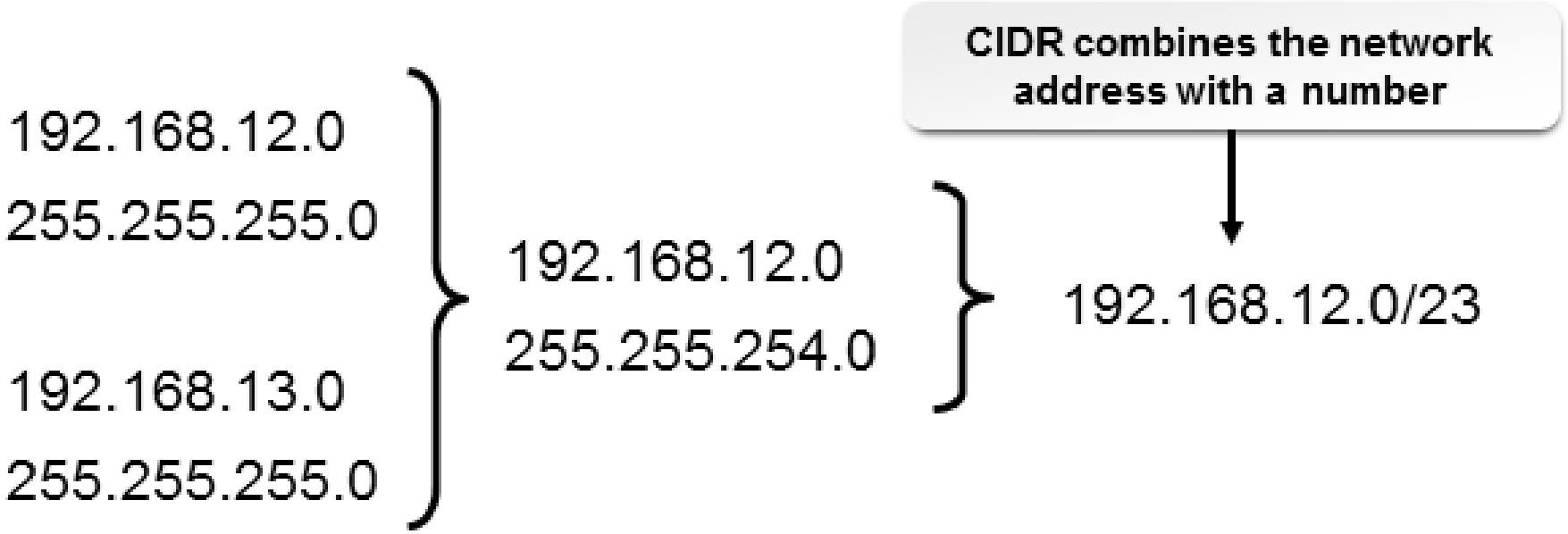
CIDR- Classless Inter-Domain Routing

- Alternative to subnetting that allows address flexibility
- No fixed dividing line between network and host
- Focuses on the number of bits used for the network address
- Class A default mask – 11111111.00000000.00000000.00000000 (/8)
- Class B default mask – 11111111.11111111.00000000.00000000 (/16)
- Class C default mask – 11111111.11111111.11111111.00000000 (/24)
- Do not have to use entire Octet of bits for Network ID
- With CIDR you can have a mask of 255.240.0.0
    - 11111111.11111000.00000000.00000000

CIDR- Classless Inter-Domain Routing

- Can be used to reference supernets
- Class C example
    - How to combine 192.168.0.0 and 192.168.1.0
    - Class C Subnet 255.255.255.0
    - But with CIDR 192.168.0.0/23
    - 1st network 11000000 - 10101000 - 00000000 - 00000000
    - 2nd network 11000000 - 10101000 - 00000001 - 00000000
    - With CIDR specifying first 23 bits
        - 255.255.254.0
        - 11111111 - 11111111 - 1111111**0** - 00000000
        - Network only blocks first 23 digits with the red digit allowing 1 or 0
- VLSM – Variable Length Subnet Mask

CIDR Further Example



CIDR- Classless Inter-Domain Routing

- http://www.subnet-calculator.com
- https://www.ultratools.com/tools/netMask
- http://www.csgnetwork.com/ipaddconv.html
- https://www.ultratools.com/tools/yourIPResult

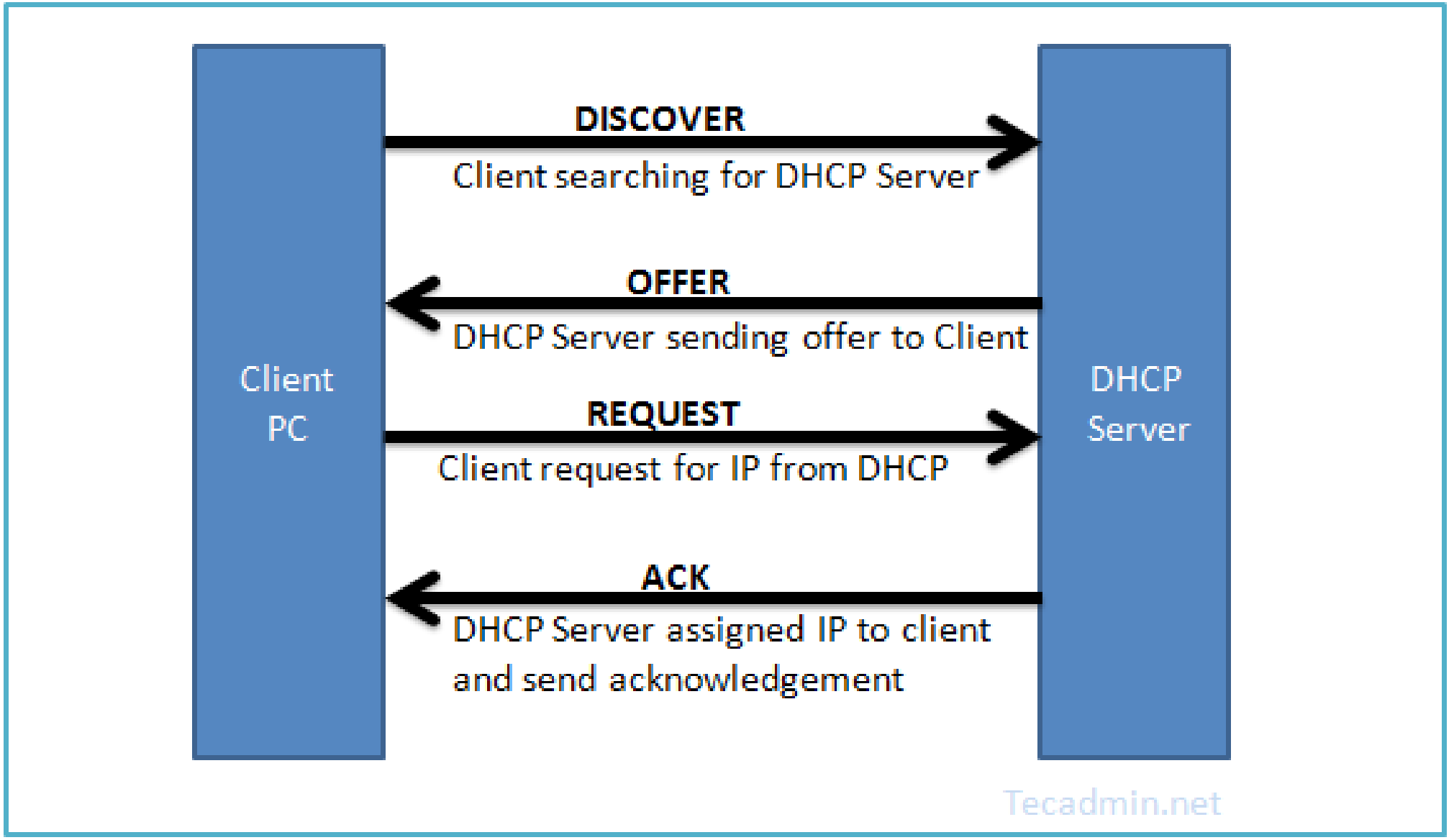
TCP/IP Choices

- Manual
  Hardest option as need to keep track. Best for small networks.
- Automatic (using DHCP). Admin sets up a scope, letting server handle all the requests. MAC addresses important for this. Best option.
- Hybrid Approach. Manual and automatic. Client pool and static IP for fixed devices. Needs careful administration.

DHCP – Dynamic Host Configuration Protocol

- DHCP – Provides IP information to a client
    - Called a **lease**.
    - Only valid for a defined period, must be renewed periodically
        - Can specify DHCP IP addresses to certain clients
    - A lease typically contains (but can do so much more)
        - IP Address
        - Subnet Mask
        - Default Gateway (Access to the WWW)
        - DNS Server address
    - Client on boot sends a broadcast called DHCP DISCOVER
    - DHCP Server responds privately
    - Alternative to Static IP addressing
        - Some equipment will have static addresses (Routers, Servers, Printers)

DHCP Request Process



DHCP Request Process

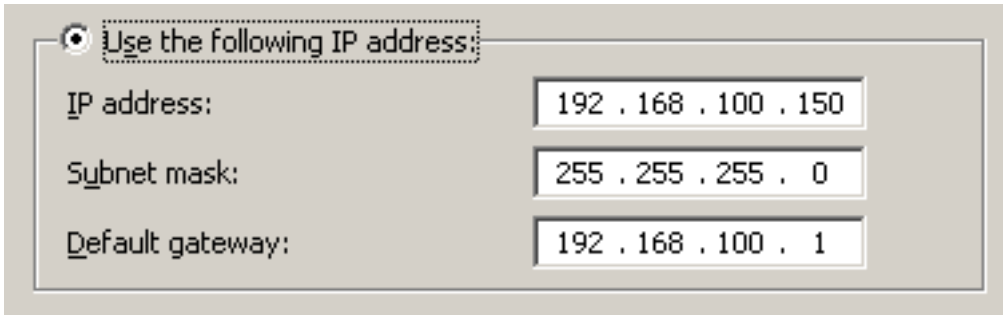
- Discover and Request are BROADCAST
    - Every computer sees the request – can slow network performance
    - Broadcast requests do not go through routers
        - Make Router DHCP Server
        - Install a DHCP Relay Agent
- Offer and Ack(nowledgement) are direct
- Uses ports 67 and 68
-
- No DHCP server then APIPA address (169.254.x.x)
    - Automatic Private IP addressing

DHCP – Dynamic Host Configuration Protocol

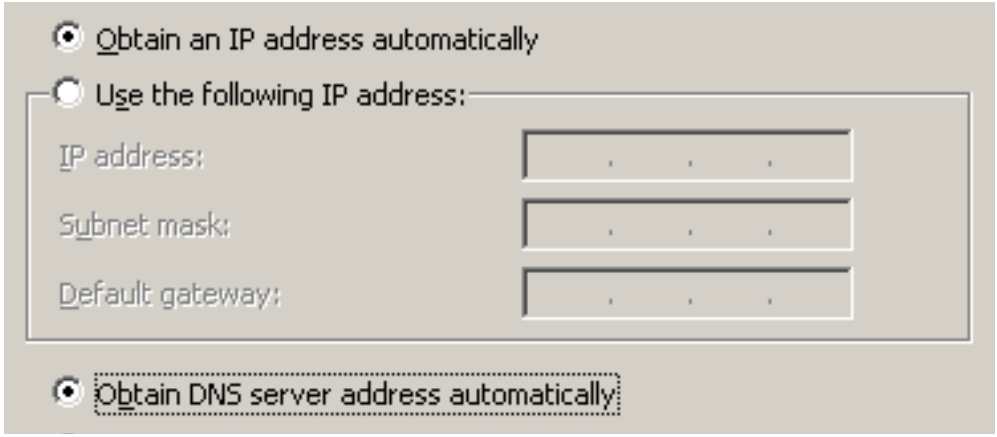
- DHCP Scopes
    - Contains information it can supply to a client
    - At least one but can have more than one
    -
    - Address Pool – Range of addresses for clients. (Need subnet mask in IPv4)
    - Lease Duration – expiry time
    - Address Reservations – Some IP addresses reserved for certain clients. Based on MAC address e.g. Printers, servers etc
    - Scope Options – Extra items such as address of default gateway, DNS Servers

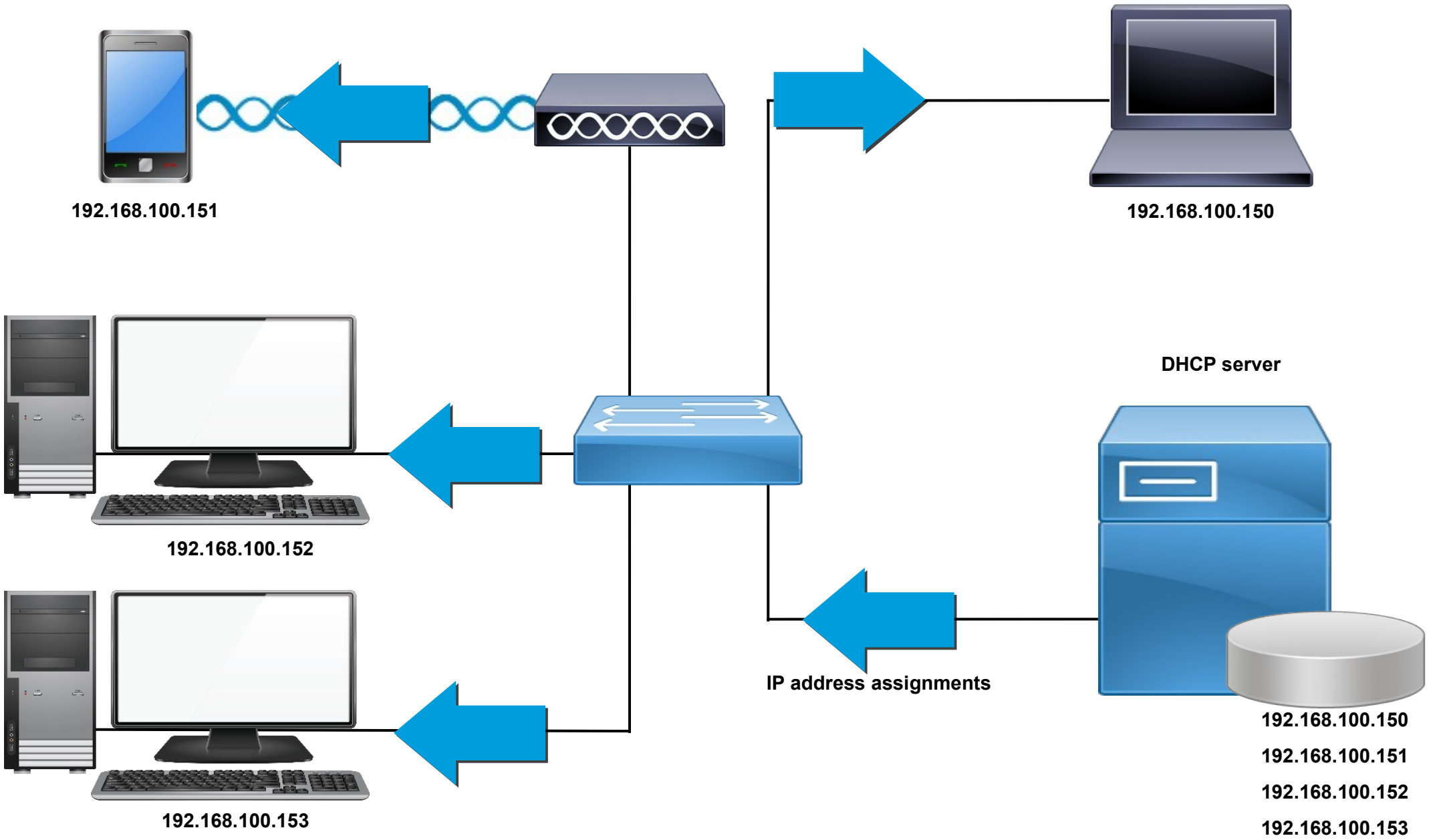
Static and Dynamic Addressing

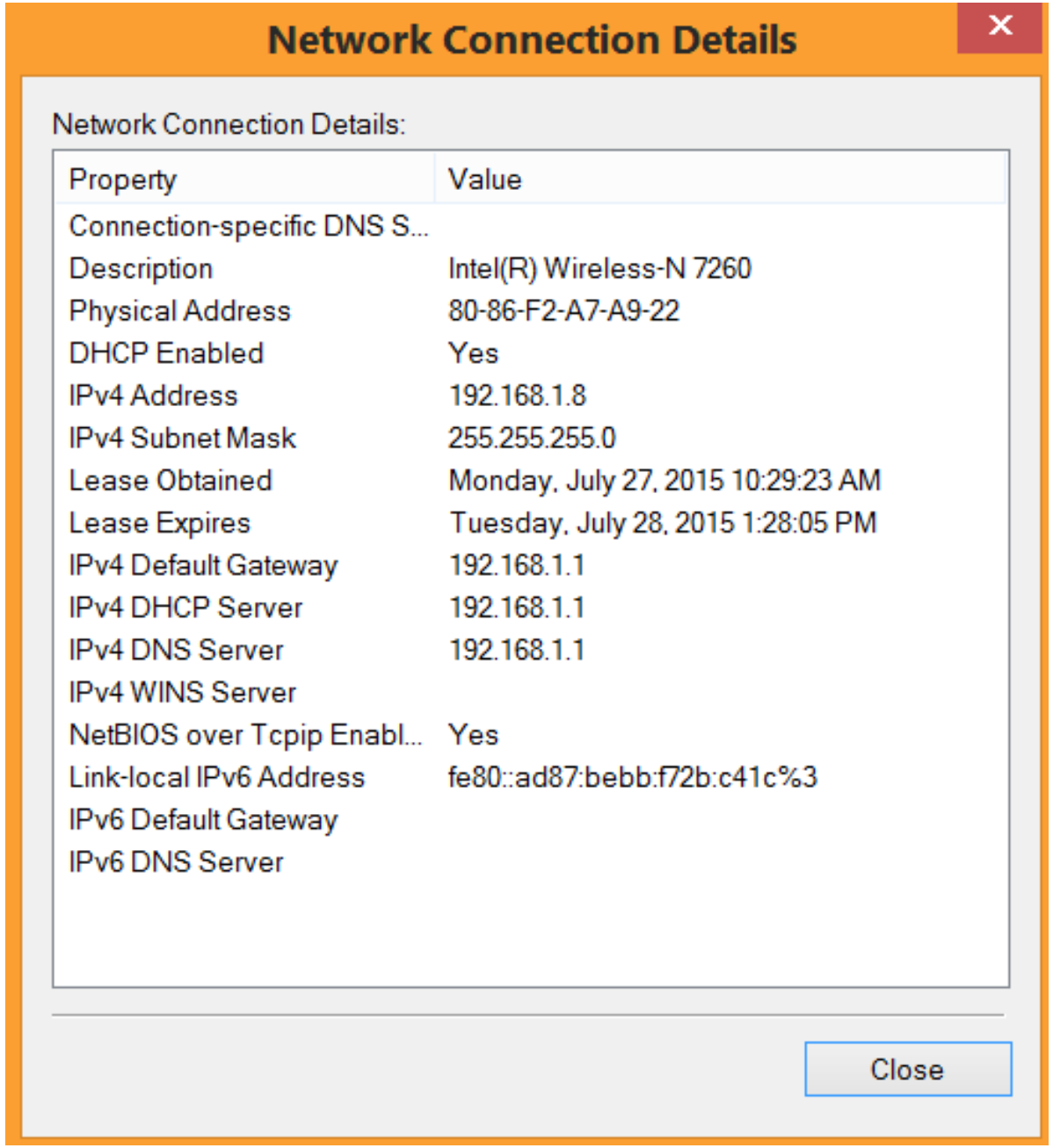
Static addressing



Dynamic addressing




192.168.100.151
192.168.100.150
DHCP server
192.168.100.152
IP address assignments
192.168.100.150
192.168.100.151
192.168.100.152
192.168.100.153
192.168.100.153


Network Connection Details
Network Connection Details:
Property
Value
Connection-specific DNS S...
Description
Intel(R) Wireless-N 7260
Physical Address
80-86-F2-A7-A9-22
DHCP Enabled
Yes
IPv4 Address
192.168.1.8
IPv4 Subnet Mask
255.255.255.0
Lease Obtained
Monday, July 27, 2015 10:29:23 AM
Lease Expires
Tuesday, July 28, 2015 1:28:05 PM
IPv4 Default Gateway
192.168.1.1
IPv4 DHCP Server
192.168.1.1
IPv4 DNS Server
192.168.1.1
IPv4 WINS Server
NetBIOS over Tcpip Enabl...
Yes
Link-local IPv6 Address
fe80::ad87:bebb:f72b:c41c%3
IPv6 Default Gateway
IPv6 DNS Server
Close

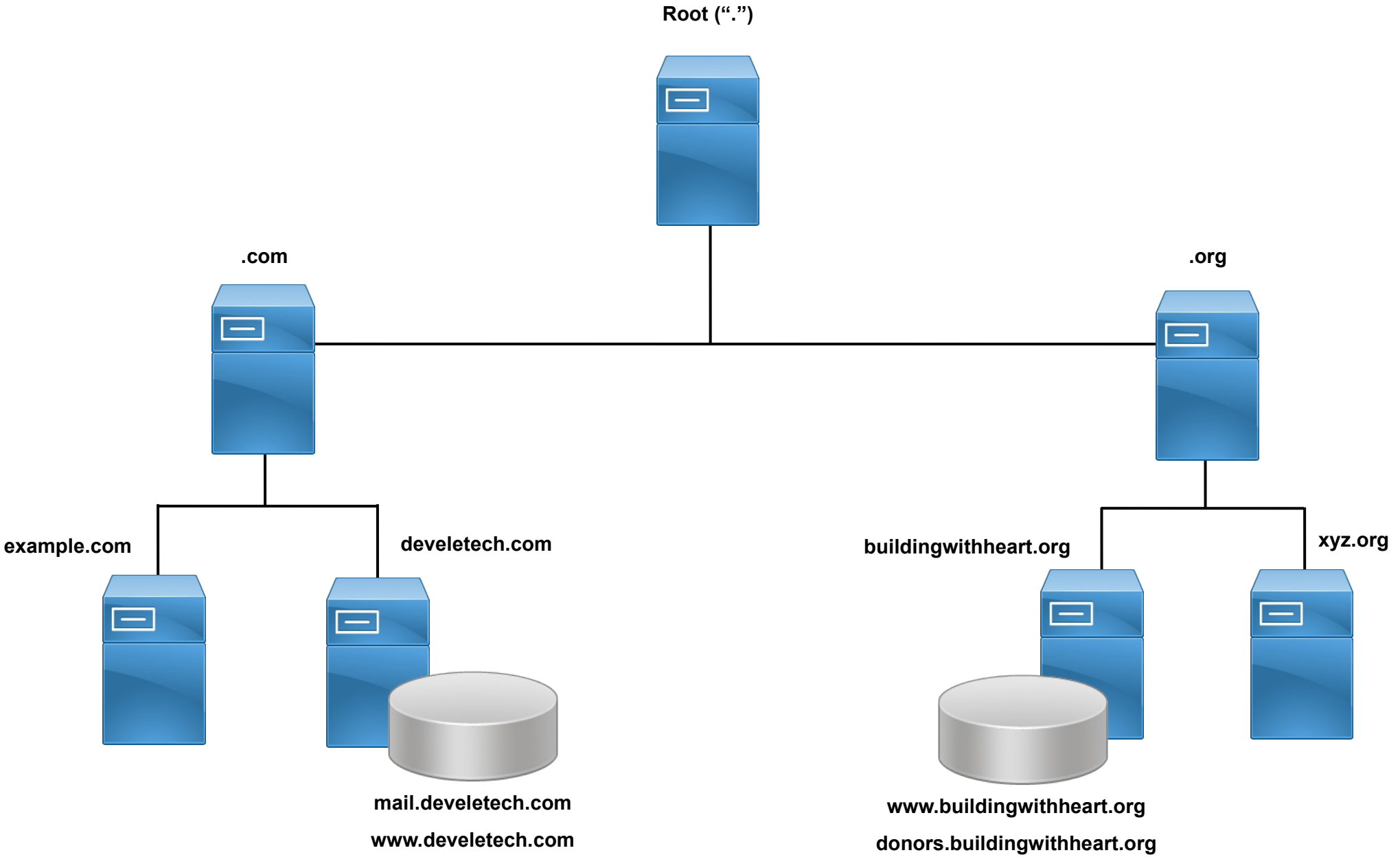
APIPA – Automatic Private IP Addressing

- Default configuration if no DHCP response
- APIPA Network 169.254.0.0 and subnet 255.255.0.0
- Immediately suspect a network problem (ipconfig confirms)

- If no need to connect to internet, all PCs will configure themselves!
- Increased broadcast traffic

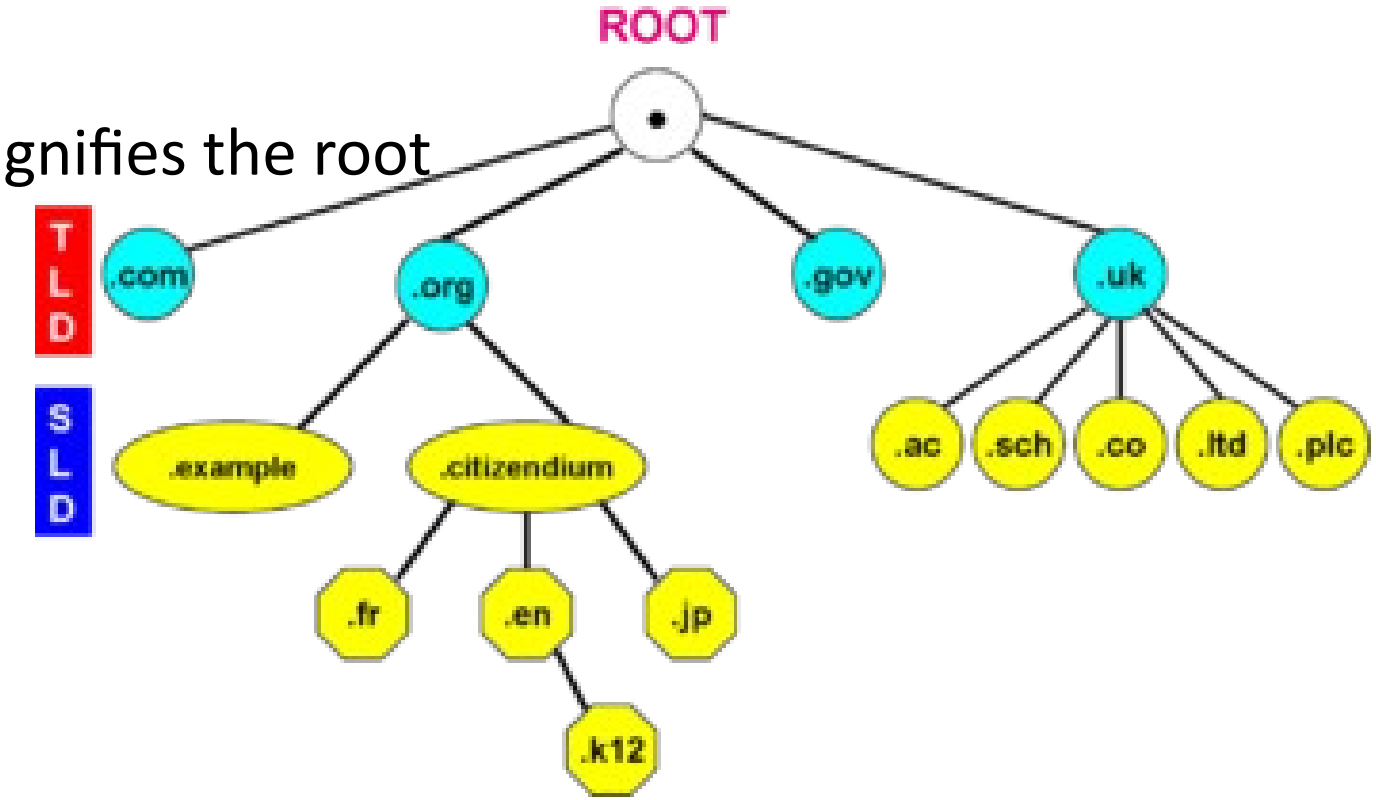
DNS – Domain Name System

- Resolves hostnames to IP Addresses
- Uses UDP or TCP port 53
- Local DNS should be placed in the DMZ
- Same on Intranet as the Internet
- ISP's maintain DNS for companies.
    - Two DNS servers needed for redundancy
- DNS Server has a *zone file*
    - (see https://en.wikipedia.org/wiki/Zone_file)
- Decides when we enter a URL where the server sits
    - Ping www.bbc.co.uk and note the IP address
    - Cascades requests upwards

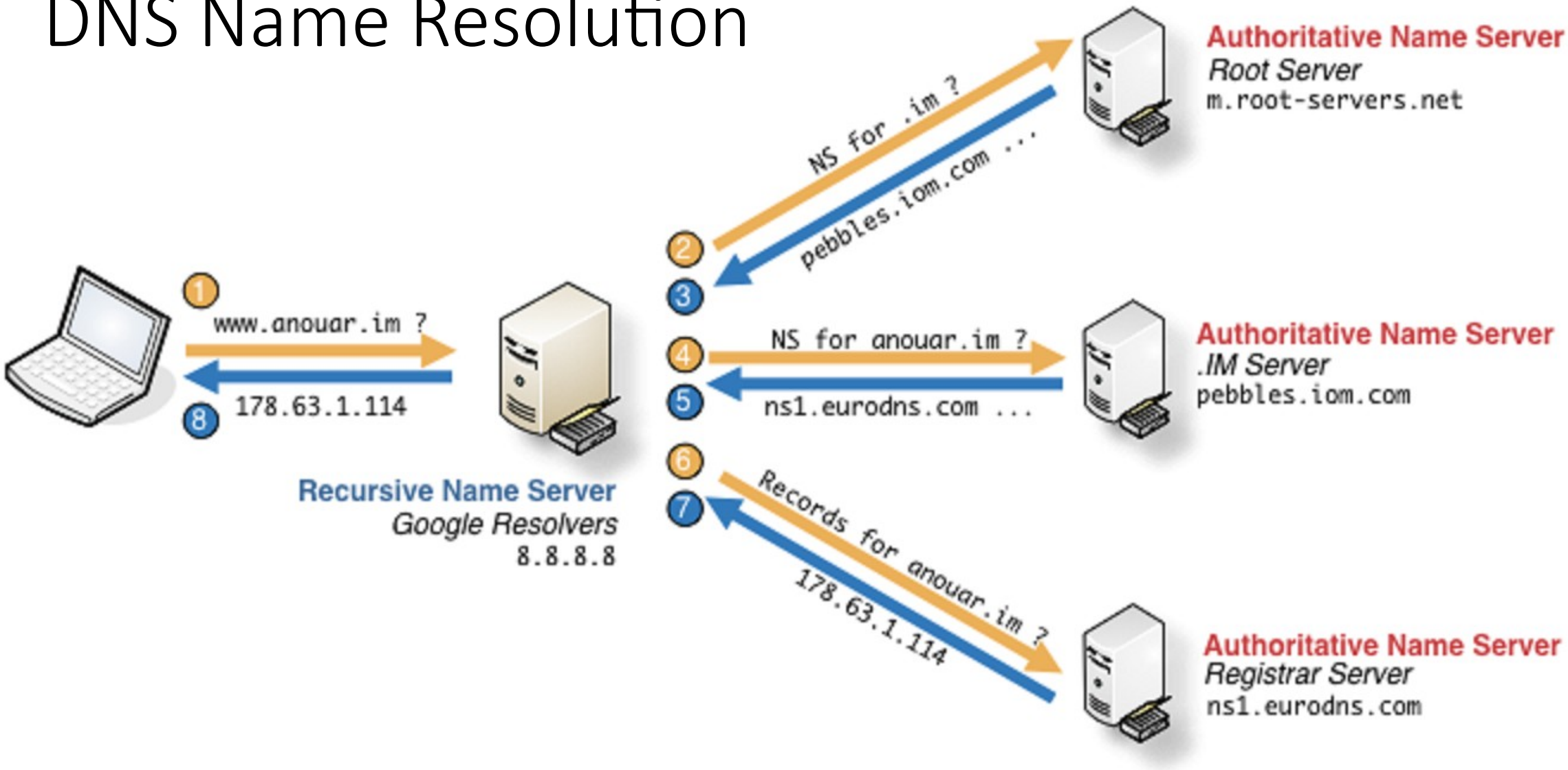

Root (“.”)
.com
.org
example.com
develetech.com
buildingwithheart.org
xyz.org
mail.develetech.com
www.develetech.com
www.buildingwithheart.org
donors.buildingwithheart.org

Internet DNS

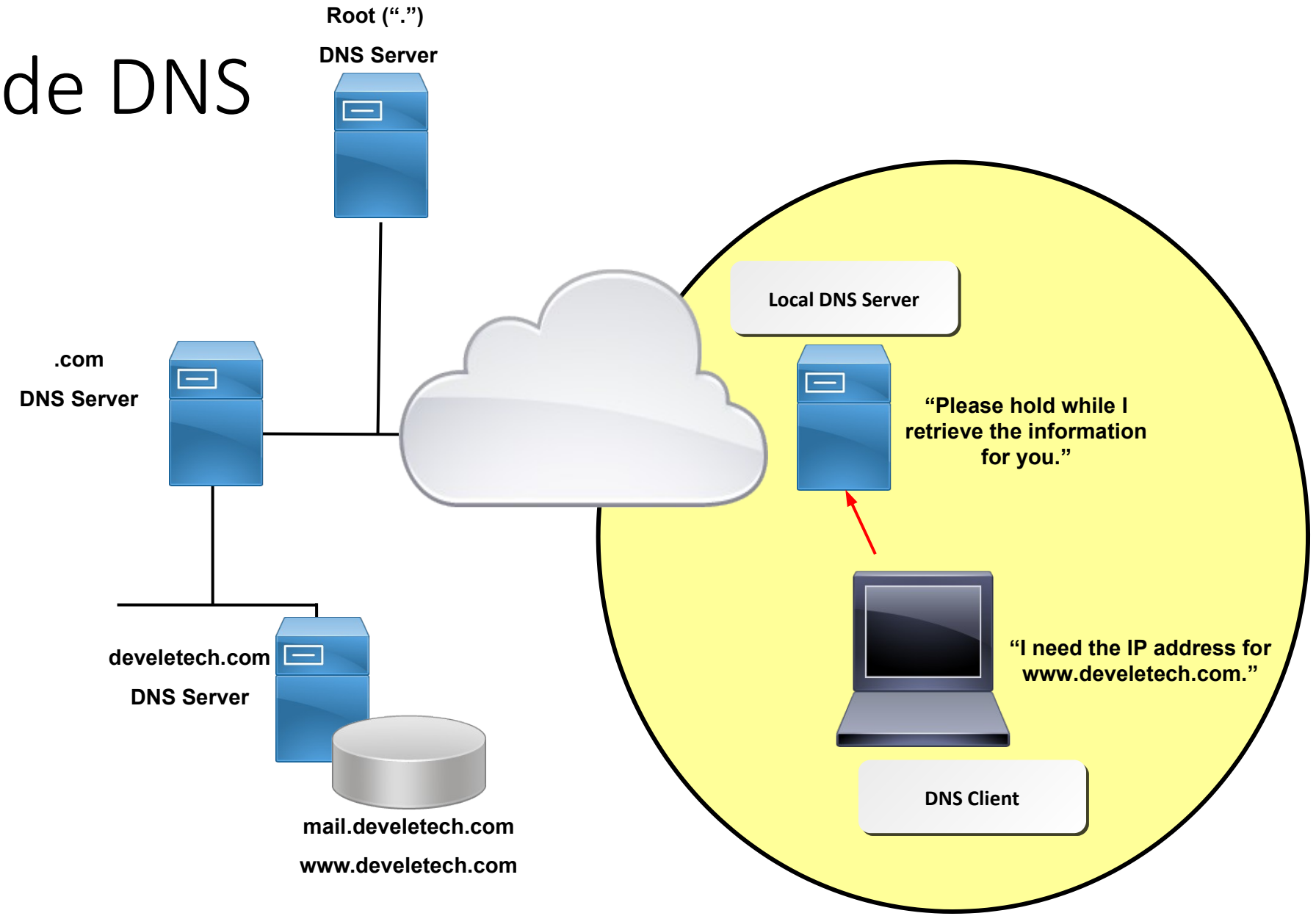
- First check zone file
- Then cache – a temporary store of recent resolved names and IP addresses
- Root Server
- Trailing dot (in first few rows) – signifies the root
    - 13 global root servers
    - TLD – top level domain
    - SLD – Second Level Domain
    - Subdomains (optional)
    - Host
- www.yahoo.com is actually www.yahoo.com.
-



DNS Name Resolution



Client Side DNS



DNS Zone File Format

- 5 Columns
    - Name of the server or computer
    - IN – means internet
    - Record Type – See next slide
    - Address of the computer
    - Comments – must have semicolon
- Managed by the DNS administrator

Zone File common DNS Record types

- SOA – Start of Authority
- NS – Name Server (Name or address of the DNS server for the zone)
- MX – Mail Exchanger (Name or address of email server)
- A – IPv4 host record
- AAAA – quad A – Host record for IPv6
- CNAME – Canonical Name. An alias to allow multiple names to be assigned to the same host or address

Public v Private IP Addresses

- All addresses on the internet are public
- Must be unique
- These IP Addresses are purchased
- Limited number of public addresses
- Therefore private addresses
    - Not exposed or routable on the internet
    - Means addresses can be repeated in differing networks
    - But given addresses are now used, how do they contact internet?

NAT – Network Address Translation

- NAT
  - Runs on a router
  - Translates internal IP addresses to external IP addresses
  - When you request resource from bbc.co.uk, the packets arrive at your PC
  - Reservations for Private IP addresses (for private, non routable IP addresses)
  - These networks are hidden from the internet

Class	IP Address Range	Default Subnet Mask	Number of Hosts
A	10.0.0.0 to 10.255.255.255	255.0.0.0	16.7 Million
B	172.16.0.0 to 172.31.255.255	255.240.0.0	1 Million
C	192.168.0.0 to 192.168.255.255	255.255.0.0	65536

IPv6

- IPv4 limitations:
  - running out of addresses!
  - Difficult to configure (Subnet and CIDR)
  - 32 bits – almost 4.3 billion addresses, but only 250 useable and taken
- IPv5 was experimental Internet Streaming Protocol
- IPv6
  - 128 bit addresses
  - 3.4×10^{38} addresses!
  - More difficult to remember
  - Easy configuration
  - Enhanced Flexibility
  - Backward compatible (seamless transition)

IPv6 Address Further example

2001:0DB8:AC10:FE01:0056:0000:0000:0000/64

An example IPv6 address

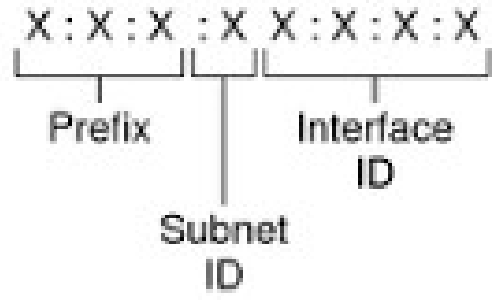
2001:0DB8:AC10:FE01:0056:0000:0000:0000

Hexadecimal format

0010 0000 0000 0001:0000 1101 1011 1000:1010 1100 0001 0000:1111 1110 0000 0001:
0000 0000 0101 0110:0000 0000 0000 0000:0000 0000 0000 0000:0000 0000 0000 0000

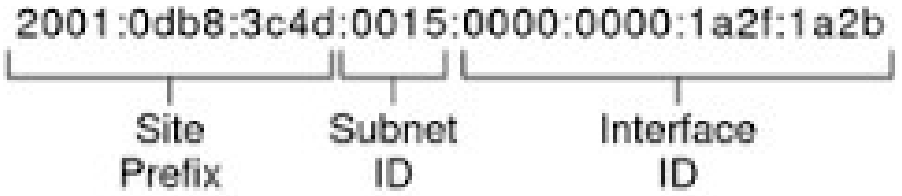
128-bit binary format

IPv6 Addressing



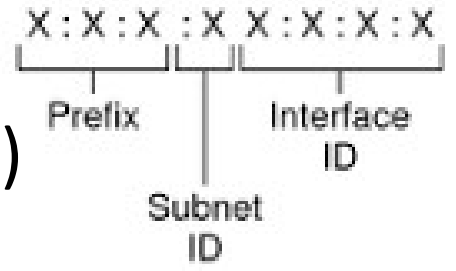
- Eight 16bit fields
- Hexadecimal Digits (not case sensitive)
- 3 Types of Address:
  - Unicast – assigned to a single node
  -
  - Anycast – assigned to multiple nodes
    Packets delivered to closest node
    One-to-nearest addressing
  -
  - Multicast – used by multiple hosts and allows communication to groups of computers

Example:

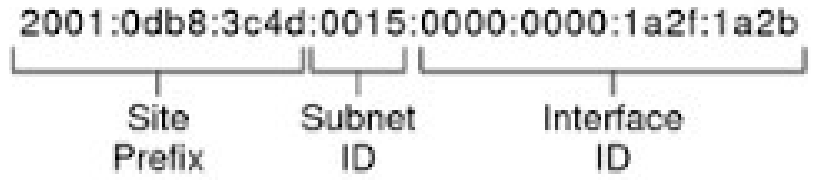


IPv6 Addressing

- No broadcast addresses (use multicast)
- A network interface can have more than one address
- First 4 fields (64 bits) network and subnetwork
  - Actually first 56 bits are routing prefix
  - Next 8 are the Subnet ID
- Last 4 fields are interface ID (like hostID on IPv4)
  - Can be created from MAC address
  - Or assigned by a DHCPv6 Server
  - Or Randomly assigned
  - Or Manually configured



Example:



IPv6 Addressing

- An IPv6 address could be written as 2001:0db8:3c4d::/48
- /48 indicates bits in routing prefix
- Long addresses
    - can eliminate zeros as follows:
        - 2001:0db8:3c4d:0012:0000:0000:1234:56ab
        - 2001:db8:3c4d:12:0:0:1234:56ab
    - can also remove consecutive groups of zeros with ::
        - 2001:0db8:3c4d:0012:0000:0000:1234:56ab
        - 2001:db8:3c4d:12::1234:56ab
        - Can only do on one group though
            - Example 2001::1ab4::5468 – what position is 1ab4 ?

Mixed v4 and v6 Networks

- IPv6 backwards compatible with IPv4
    - sets first 80 bits to zero
    - next 16 bits to 1
    - Final 32 to the IPv4 address
    - Example IPv6 address on IPv4 network - ::ffff:192.168.1.19

IPv6 Reserved Addresses

- IPv6 APIPA
    - All IPv6 must have a Local Link Address
    - fe80::/10
    - Non routable
- Loopback Address (IPv4 127.0.0.1)
    - ::1/128 (written as ::1)
- Global Addresses (for internet use)
    - 2000::/3
- Multicast Address
    - FF00::/8

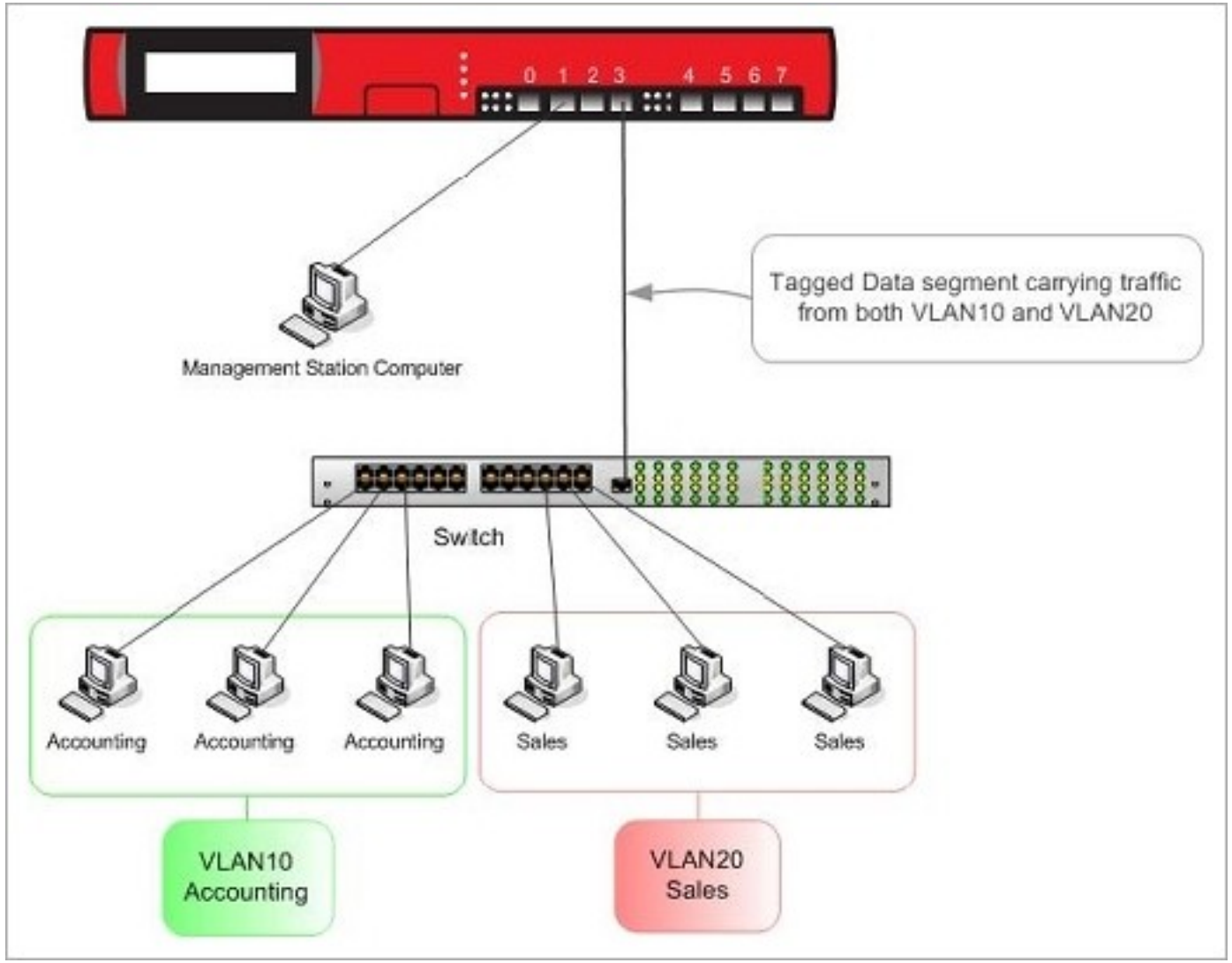
IPv6 Address Ranges

Address	Use
0:0:0:0:0:0:0:0	Can be written as :: Equivalent to 0.0.0.0 in IPv4. Means host is not configured.
0:0:0:0:0:0:0:1	Can be written as ::1 Equivalent to 127.0.0.1 in IPv4.
2000::/3	Global Unicast address range for use on the internet
FC00::/7	Unique local unicast address range
FE80::/10	Link local unicast range
FF00::/8	Mulitcast range

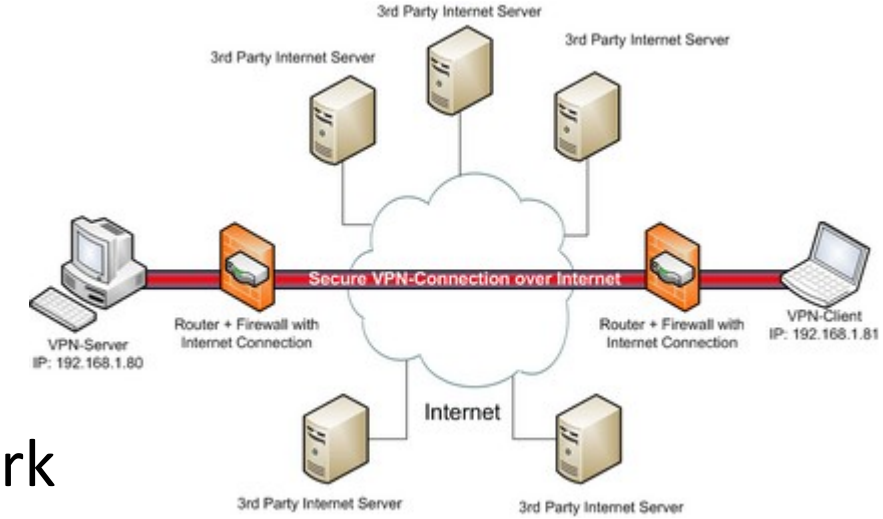
Virtual Networks

- Two types:
  - Virtual Local Area Network
  - Virtual Private Network
- VLANs created by using a managed switch
  - STP (Spanning tree protocol)
  - STP ensures no infinite network loops (data being sent between switches)
- VLAN Benefits
  - Broadcast Traffic is reduced
  - Security is increased
  - PC’s in multiple locations can all belong to the same VLAN
  - Reconfiguration is easy

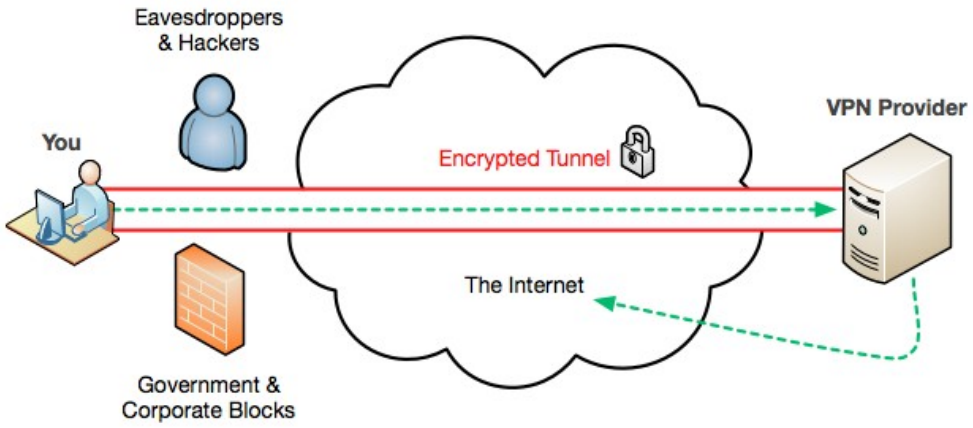
Virtual Networks



Virtual Networks



- Virtual Private Networks
  - Allows remote users to be on internal network
  - Data is TUNNELLED from client PC using encapsulation and encryption
  - Allows two networks to be joined as if local
  - Requires dedicated hardware or software
  - WIN 10 includes VPN software
    - Start > Settings > Network&Internet > VI



Exam Essentials

- IPv4 Addressing
    - 32 bit
    - Four octet notation
    - Needs a Subnet mask
    - Subnet Mask octet notation
- IPv6 Addressing
    - 128 bit addresses
    - Eight fields of four hex characters
    - Shorthand notations

Exam Essentials

- Know about DHCP and DNS
- Know common TCP/IP ports
    - HTTP, FTP, POP3, SMTP, Telnet, HTTPS
- Identify IP address classes A, B and C
- Know the private IP addresses ranges
    - 10.0.0.0/8
    - 172.16.0.0/16
    - 192.168.0.0/16
- Know the APIPA range 169.254.0.0/16
    - No APIPA in IPv6

Exam Essentials

- Know IPv6 three types of addresses
    - Unicast – single node on network
    - Anycast – for a small group of systems, delivery to the closest node
    - Multicast – delivers to all computers in a group
- Recognise IPv6 Special addresses