

*CS 07351 –
Cybersecurity: Fundamentals, Principles, and Applications*

Week 2 - 3

Any questions from the previous week?

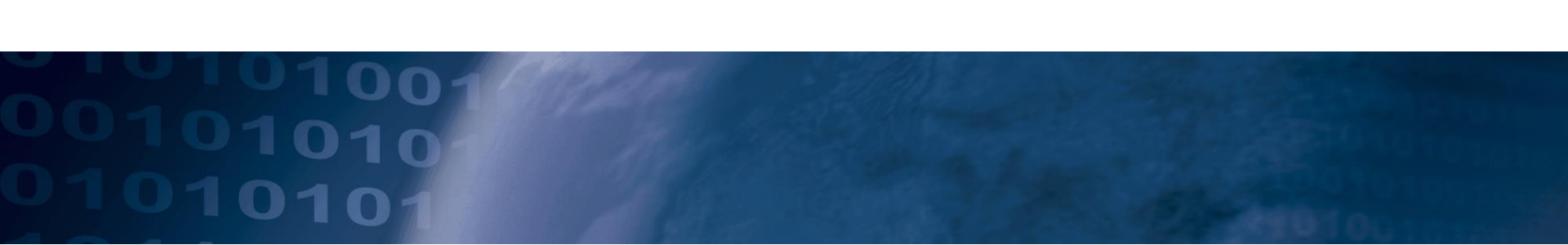
Continue Chp1 (OSI Model)

Chp 2 & 3



TQXXA OXMEE

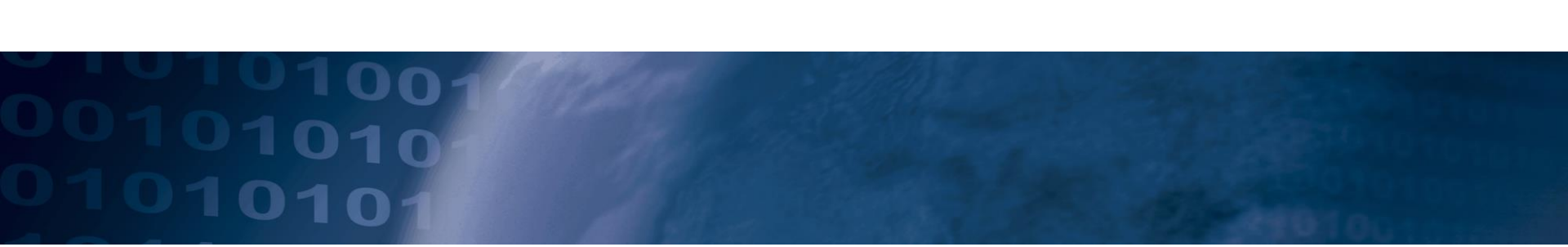
TAI MDQ KAG PAUZS, FTQ
RAGZPMFUAZ AR FTUE OXMEE UE
NMEQP AZ FTQ OUM FDUMP -
OAZRUPQZFUMXUFK, UZFQSDUFK MZP
MHMUXMNUXUFK. FTMZW KAG



https://www.simonsingh.net/The_Black_Chamber/caesar.html
(Caesar Cipher – 12)

- <http://www.xarg.org/tools/caesar-cipher/> (+13)
- Uryyb pynff, Ubj ner lbh qbvat?
- Jung vf gur sbhaqngvba bs Vasbezngvba Frphevgl?
- pbasvqragvnyvgl vagrtevgl naq ninvynovyvgl
- <http://www.guballa.de/substitution-solver>
- pbasvqragvnyvgl vagrtevgl naq ninvynovyvgl
- Wrong cipher produce wrong results
- <http://www.dcode.fr/caesar-cipher> (+3)
- Fubswrjudskb lv d phwkrq ri vwrulqj dqg wudqvplwwlqj gdwd lq d sduwlfxodu irup vr wkdw rqob wkrvh iru zkrp lw lv lqwhqghg fdq uhdg dqg surfhvv lw.

- <https://crackstation.net/>
 - <http://www.md5hashgenerator.com/>
 - <https://passwordsgenerator.net/sha256-hash-generator/>
 - <https://passwordsgenerator.net/sha1-hash-generator/>
 - <http://onlinemd5.com/>
-
- <https://hashes.org/public.php>
 - <https://crackstation.net/>
 - <https://hashcat.net/hashcat/>
 - <http://www.md5hashgenerator.com/>
 - <http://aesencryption.net/>
 - <http://www.xarg.org/tools/caesar-cipher/>
 - <http://www.guballa.de/substitution-solver>
 - <http://quipqiup.com/>
 - http://www.simonsingh.net/The_Black_Chamber/index.html
 - http://www.cryptool-online.org/index.php?option=com_content&view=article&id=47&Itemid=29&lang=en
 - <http://www.dcode.fr/caesar-cipher>
 - https://www.simonsingh.net/The_Black_Chamber/index.html

The header of the slide features a dark blue background. On the left side, there are several lines of binary code (0s and 1s) in a lighter blue color. To the right of the binary code, there is a faint, glowing image of a globe or a network map, suggesting a global network theme.

How many Total Ports are available
within the Internet/Network?



65535 ports

Well Known Ports: 0 through 1023.

Registered Ports: 1024 through 49151.

Dynamic/Private : 49152 through 65535

Ports

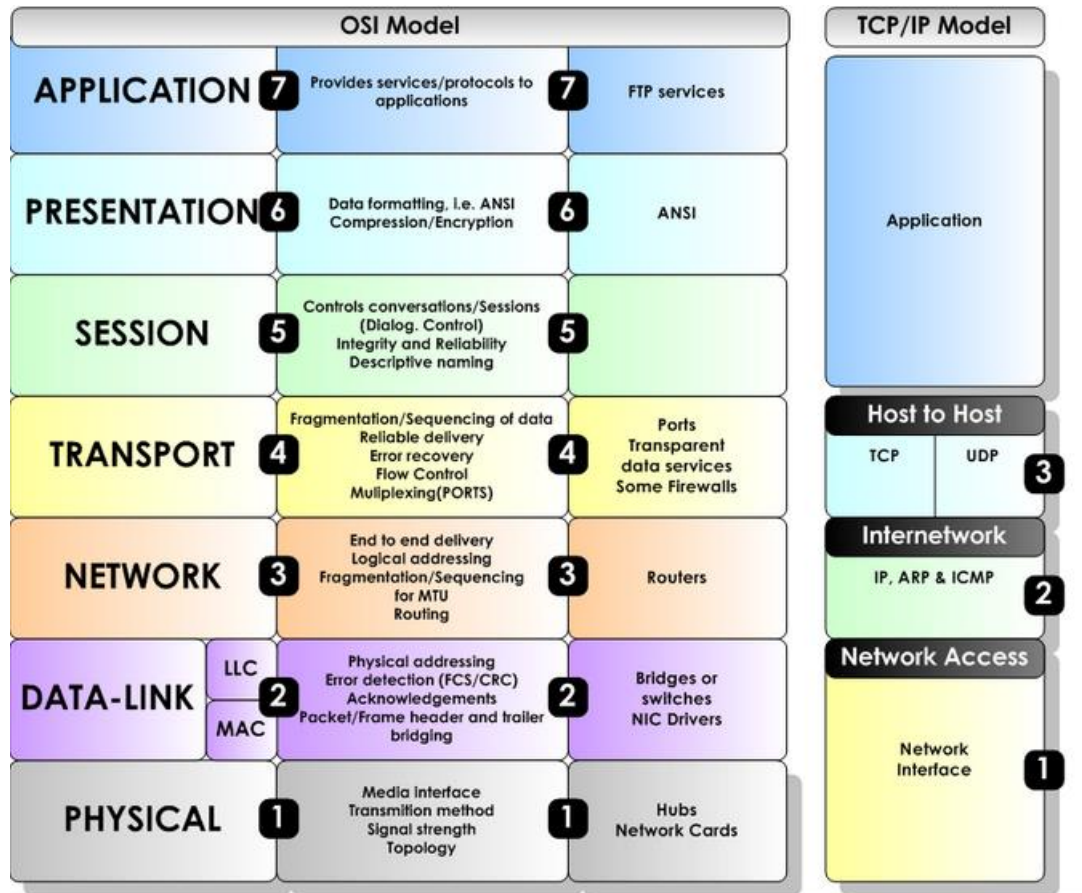
Port	TCP Port Assignment	UDP Port Assignment
21	FTP	
22	SSH	
25	SMTP	
53	DNS	DNS
80	HTTP	
110	POP3	
139	NetBIOS	
143	IMAP	
443	HTTPS	
3389	RDP	RDP

OSI Model

OSI (Open Source Interconnection) 7 Layer Model

Layer	Application/Example	Central Device/ Protocols	DOD4 Model
Application (7) Serves as the window for users and application processes to access the network services.	End User layer Program that opens what was sent or creates what is to be sent Resource sharing • Remote file access • Remote printer access • Directory services • Network management	User Applications SMTP	Process
Presentation (6) Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network.	Syntax layer encrypt & decrypt (if needed) Character code translation • Data conversion • Data compression • Data encryption • Character Set Translation	JPEG/ASCII EBDIC/TIFF/GIF PICT	
Session (5) Allows session establishment between processes running on different stations.	Synch & send to ports (logical ports) Session establishment, maintenance and termination • Session support - perform security, name recognition, logging, etc.	Logical Ports RPC/SQL/NFS NetBIOS names	
Transport (4) Ensures that messages are delivered error-free, in sequence, and with no losses or duplications.	TCP Host to Host, Flow Control Message segmentation • Message acknowledgement • Message traffic control • Session multiplexing	PACKET FILTERING TCP/SPX/UDP	Host to Host
Network (3) Controls the operations of the subnet, deciding which physical path the data takes.	Packets ("letter", contains IP address) Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting		Internet
Data Link (2) Provides error-free transfer of data frames from one node to another over the Physical layer.	Frames ("envelopes", contains MAC address) [NIC card — Switch — NIC card] (end to end) Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control	Switch Bridge WAP PPP/SLIP	Network
Physical (1) Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	Physical structure Cables, hubs, etc. Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts	Hub	

OSI Model-TCP Model



Hacked Information

- <https://pastebin.com/ub7AEpew>
- <https://pastebin.com/3PZws0N5>
- <https://pastebin.com/09KBfSE4>
- <https://pastebin.com/xTwMqEGs>

CS 07351 – *Cybersecurity: Fundamentals, Principles, and Applications* Chapter 2

Firewall main purpose is to control traffic. The firewall achieves this traffic control using Access Control Lists (ACL).

An ACL is a list of rules with permit or deny statements to a firewall interface, either on the inbound or on the outbound traffic direction. If the ACL is applied on the inbound traffic direction (in), then the ACL is applied to traffic entering a firewall interface. The opposite happens for ACL applied to the outbound (out) direction.

The ACL permit or deny statements basically consist of source and destination IP addresses and ports. A permit ACL statement allows the specified source IP address/network to access the specified destination IP address/network. The opposite happens for deny ACL statements. **At the end of the ACL, the firewall inserts by default an implicit DENY ALL statement rule which is not visible in the configuration.**

The basic command format of the Access Control List is the following:

```
ciscoasa(config)# access-list "access_list_name" extended {deny | permit} protocol "source_address" "mask" [source_port] "dest_address" "mask" [dest_port]
```

To apply the ACL on a specific interface use the access-group command as below:

```
ciscoasa(config)# access-group "access_list_name" [in|out] interface "interface_name"
```

Example 1:

Allow only http traffic from inside network 10.0.0.0/24 to outside internet

```
ciscoasa(config)# access-list HTTP-ONLY extended permit tcp 10.0.0.0 255.255.255.0 any eq 80
```

```
ciscoasa(config)# access-group HTTP-ONLY in interface inside
```

Firewall Rule Generator

<https://staff.washington.edu/corey/fw/fw.cgi>

CS 07351 – *Cybersecurity: Fundamentals, Principles, and Applications* Chapter 2

Example 2:

Deny telnet traffic from host 10.1.1.1 to host 10.2.2.2 and allow everything else.

```
ciscoasa(config)# access-list DENY-TELNET extended deny tcp host 10.1.1.1 host 10.2.2.2 eq 23
```

```
ciscoasa(config)# access-list DENY-TELNET extended permit ip host 10.1.1.1 host 10.2.2.2
```

```
ciscoasa(config)# access-group DENY-TELNET in interface inside
```

The above example ACL (DENY-TELNET) contains two rule statements, one deny and one permit. As we mentioned above, the “access-group” command applies the ACL to an interface (either to an inbound or to an outbound direction).

Example 3:

The example below will deny ALL TCP traffic from our internal network 192.168.1.0/24 towards the external network 200.1.1.0/24. Also, it will deny HTTP traffic (port 80) from our internal network to the external host 210.1.1.1. All other traffic will be permitted from inside.

```
ciscoasa(config)# access-list INSIDE_IN extended deny tcp 192.168.1.0 255.255.255.0 200.1.1.0  
255.255.255.0
```

```
ciscoasa(config)# access-list INSIDE_IN extended deny tcp 192.168.1.0 255.255.255.0 host 210.1.1.1 eq 80
```

```
ciscoasa(config)# access-list INSIDE_IN extended permit ip any any
```

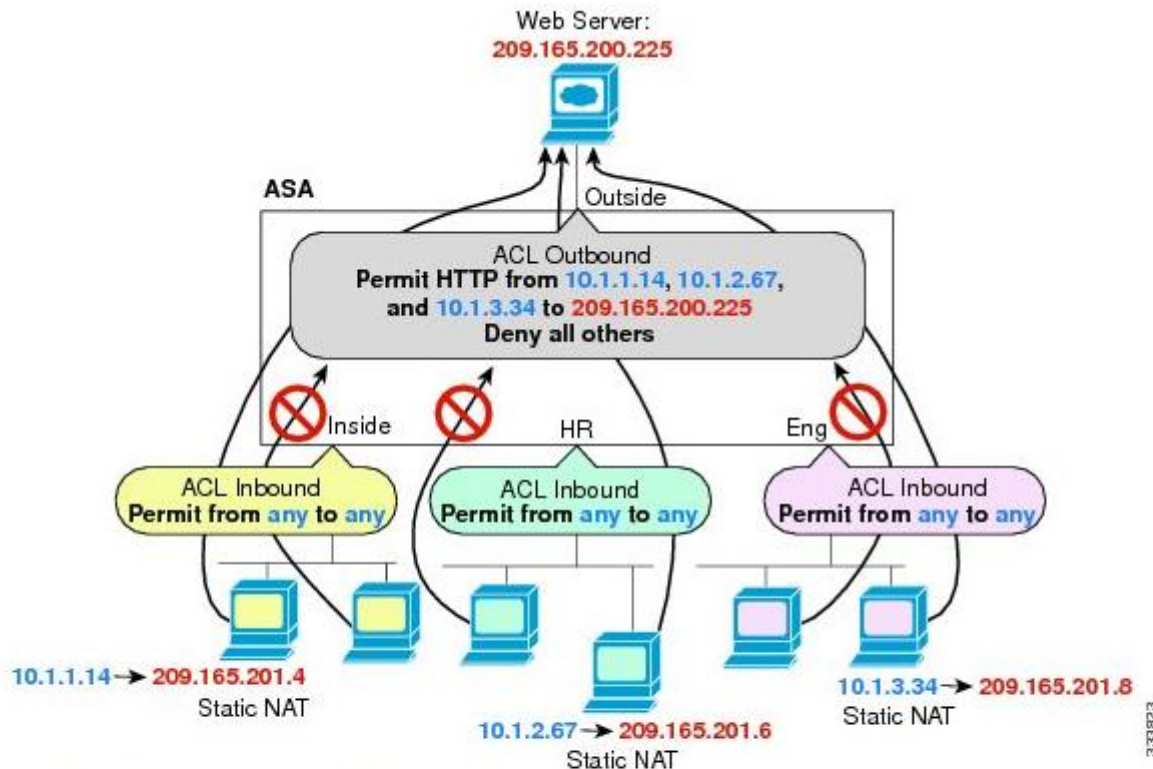
So question is what IP addresses are rules applied too?

This is where we get out our handy dandy IP calculator

<http://www.gregthatcher.com/Papers/IT/SubnetCalculator.aspx>

<http://mxtoolbox.com/subnetcalculator.aspx>

CS 07351 – *Cybersecurity: Fundamentals, Principles, and Applications*



See the following commands for this example:

```
ciscoasa(config)# access-list OUTSIDE extended permit tcp host 10.1.1.14 host 209.165.200.225 eq www
ciscoasa(config)# access-list OUTSIDE extended permit tcp host 10.1.2.67 host 209.165.200.225 eq www
ciscoasa(config)# access-list OUTSIDE extended permit tcp host 10.1.3.34 host 209.165.200.225 eq www
ciscoasa(config)# access-group OUTSIDE out interface outside
```

CS 07351 – *Cybersecurity: Fundamentals, Principles, and Applications*

Center of Internet Security – Security Benchmarks
Best Practices for configuring Firewall, Switches, etc.

WHEN CONFIGURING A FIREWALL **NEVER USE ANY, ANY**

Let's look at some best practices

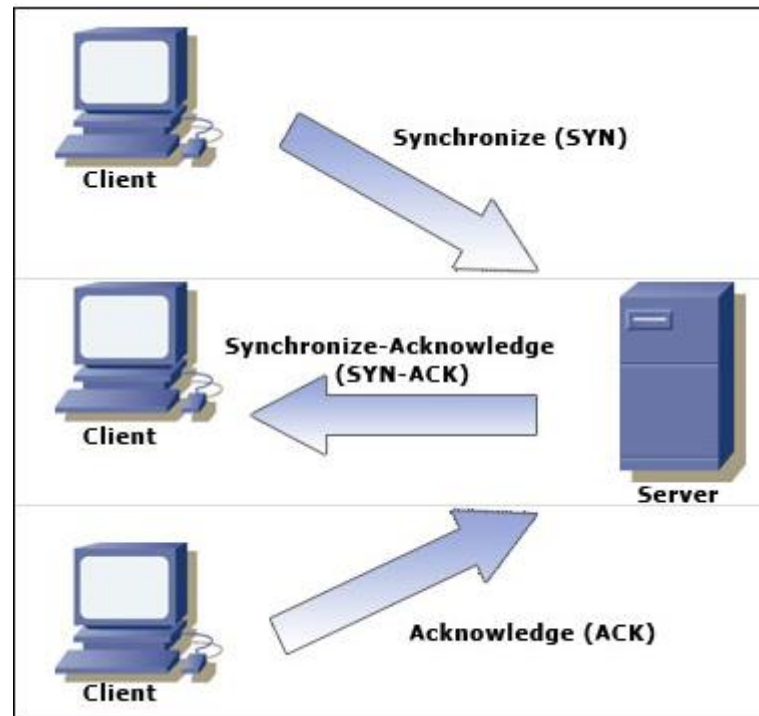
Basic Connectivity Protocols

- TCP (Transmission Control Protocol)
- UDP (User Datagram Protocol)
- IP (Internet Protocol)
- ICMP (Internet Control Message Protocol)
- ARP (Address Resolution Protocol)
- NDP (Neighbor Discovery Protocol)

TCP

- Connection-oriented: guaranteed delivery
- Three-way handshake
 - SYN
 - SYN/ACK
 - ACK
- SYN Flood Attack/Ping of Death
 - Consumes server resources, creating a Denial of Service (DoS)

CS 07351 – *Cybersecurity: Fundamentals, Principles, and Applications*



CS 07351 – Cybersecurity: Fundamentals, Principles, and Applications

This is why understanding the OSI model is important.
ICMP operates at Layer 3 because it uses an IP address
ARP operates at Layer 2 because it uses the MAC address

ex. Ping of Death – from a command prompt ping (ip address) -t -l 65510

- t manually stop it

- l size of the packet

UDP

- Connectionless
- No handshake
- No guarantee of delivery
- Often used for DoS attacks

IP

- Delivers packets to specified computer by IP Address
- IPv4: 32-bit address
 - 192.168.1.1
- IPv6: 128-bit address
 - fe80:0:0:0:462a:60ff:fef6:278a

ICMP

- Connectivity tests
 - Ping
 - Pathping
 - Tracert
- Used in DoS attacks

ARP

- Finds MAC address from IP address
- ARP Poisoning
 - Sends false ARP messages
 - Redirects traffic on a LAN
 - Commonly used for Man-In-The-Middle Attacks
 - Tool for Windows –
 - Cain and Abel <http://www.oxid.it/cain.html>
 - Nighthawk <https://code.google.com/p/nighthawk/downloads/list>
 - Command/Tools for Linux/Unix
 - arpspoof
 - To ARP Spoof the victim;
 - arpspoof -i <interface> -t <target IP> <gateway IP>
 - To ARP Spoof the gateway router;
 - arpspoof -i <interface> -t <gateway IP> <target IP>

IP Address Classes

- IP addresses are divided into 5 classes, each of which is designated with the alphabetic letters A to E.
- Class D addresses are used for multicasting.
- Class E addresses are reserved for testing & some mysterious future use.

CS 07351 – Cybersecurity: Fundamentals, Principles, and Applications

Class	1 st Octet Decimal Range	1 st Octet High Order Bits	Network/Host ID (N=Network, H=Host)	Default Subnet Mask	Number of Networks	Hosts per Network (Usable Addresses)
A	1 – 126*	0	N.H.H.H	255.0.0.0	126 ($2^7 - 2$)	16,777,214 ($2^{24} - 2$)
B	128 – 191	10	N.N.H.H	255.255.0.0	16,382 ($2^{14} - 2$)	65,534 ($2^{16} - 2$)
C	192 – 223	110	N.N.N.H	255.255.255.0	2,097,150 ($2^{21} - 2$)	254 ($2^8 - 2$)
D	224 – 239	1110	Reserved for Multicasting			
E	240 – 254	1111	Experimental; used for research			

Note: Class A addresses 127.0.0.0 to 127.255.255.255 cannot be used and is reserved for loopback and diagnostic functions.

Private IP Addresses

Class	Private Networks	Subnet Mask	Address Range
A	10.0.0.0	255.0.0.0	10.0.0.0 - 10.255.255.255
B	172.16.0.0 - 172.31.0.0	255.240.0.0	172.16.0.0 - 172.31.255.255
C	192.168.0.0	255.255.0.0	192.168.0.0 - 192.168.255.255

IP Address Classes

- Using the ranges, you can determine the class of an address from its 1st octet value.
- An address beginning with 120 is a Class A address, 155 is a Class B address & 220 is a Class C address.

Octets

- The 32-bit IP address is broken up into 4 octets, which are arranged into a dotted-decimal notation scheme.
- An octet is a set of 8
- Example of an IP version 4:
172.64.126.52

Thinking in Binary

- To most humans, the number 124 represents $100 + 20 + 4$.
- To the computer, this number is 01111100, which is $64 (2^6) + 32 (2^5) + 16 (2^4) + 8 (2^3) + 4 (2^2) + 0 + 0$

Converting to Decimal

- Now what is its equivalent decimal value?

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

The binary number 1111 1111 converts into the decimal number:

$$128 + 64 + 32 + 16 + 8 + 4 + 2 + 1 = 255$$

Converting to Decimal

- Therefore, the largest decimal number that can be stored in an IP address octet is 255.

Locating your IP Address

- Can you tell me your IP address of your laptop, tablet, smartphone?

Question

We also know that the default standard Class C subnet mask is: 255.255.255.0
What is the binary equivalent?

*CS 07351 –
Cybersecurity: Fundamentals, Principles, and Applications*

11111111.11111111.11111111.00000000

Subnetting at high level

- Subnetting is the process of dividing a network & its IP addresses into segments, each of which is called a subnetwork or subnet.
- There are 2 fundamental reasons why subnetting has so much importance in today's networking environment:

Subnetting cont.

- 1) The world is running out of available IP version 4 addresses and subnetting helps extend the existing addresses

Subnetting cont.

- 2) Subnetting reduces the size of the routing tables stored in routers. Subnetting extends the existing IP address base & restructures the IP address. As a result, routers must have a way to extract from a IP address both the Network address & the Host address.

Subnetting cont.

- Example of subnetting: when the network administrator divides the 172.20.0.0 network into 5 smaller networks – 172.20.1.0, 172.20.2.0, 172.20.3.0, 172.20.4.0 & 172.20.5.0 – the outside world stills sees the network as 172.20.0.0, but the internal routers now break the network addressing into the 5 smaller subnetworks.

Subnetting cont

- In the example, only a single IP address is used to reference the network & instead of 5 network addresses, only one network reference is included in the routing tables of routers on other networks.

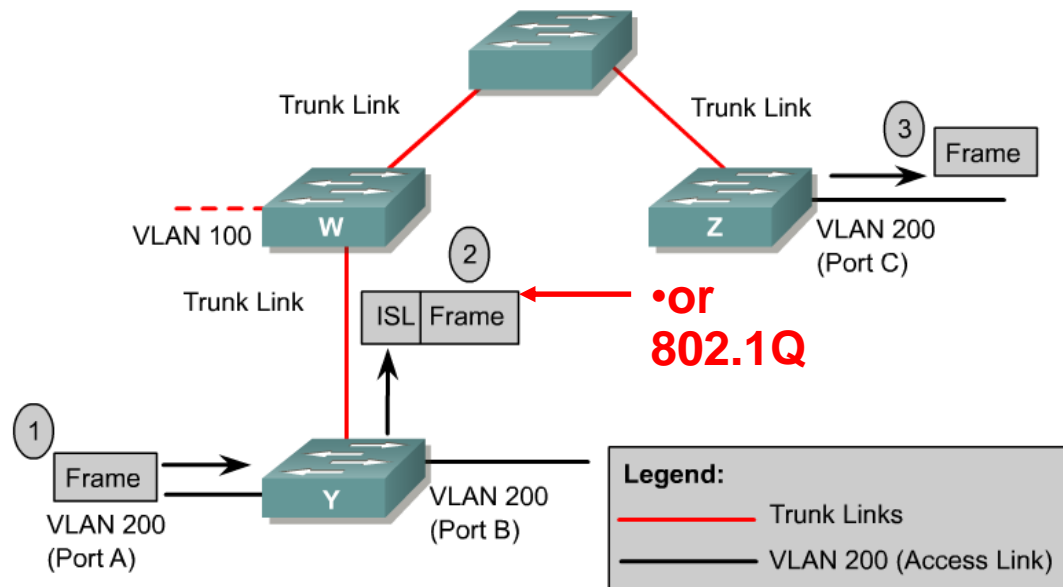
Borrowing Bits in Subnetting

- The key concept in subnetting is borrowing bits from the host portion of the network to create a subnetwork.
- The rules require that two bits remain available to use for the Host ID & that all of the subnet bits cannot be all 1s or 0s at the same time.

Borrowing Bits in Subnetting cont.

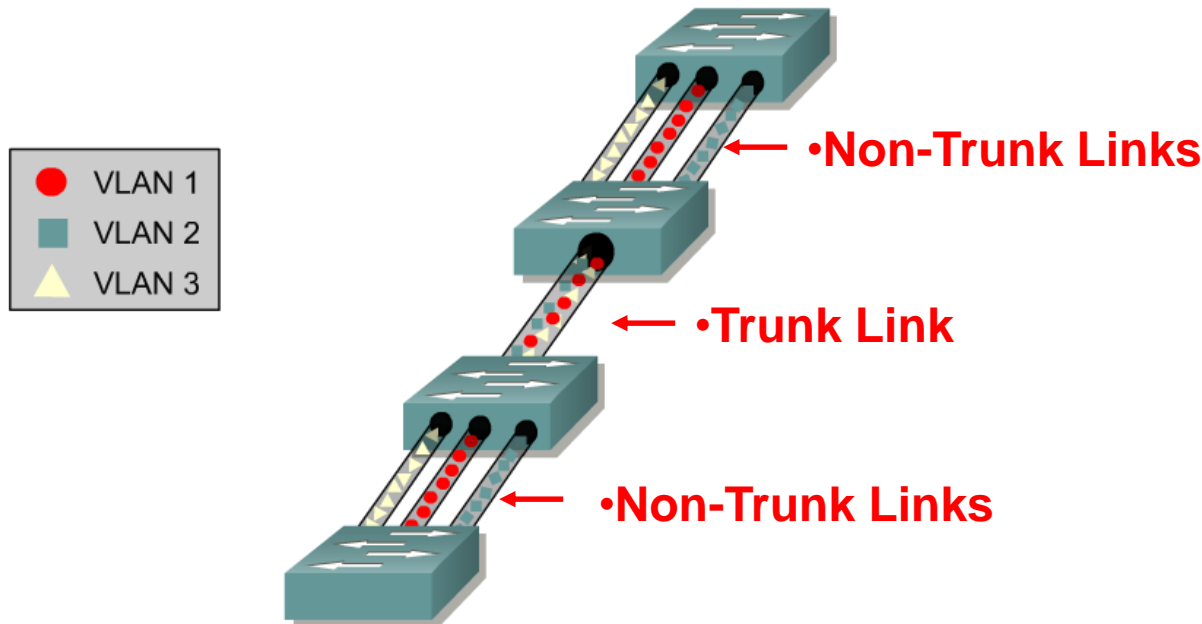
•Bits Available for Creating Subnets		
•Address Class	•Host Bits	•Bits Available for Subnet
•A	•24	•22
•B	•16	•14
•C	•8	•6

Trunking



- Trunking protocols were developed to effectively manage the transfer of frames from different VLANs on a single physical line.
- The trunking protocols establish agreement for the distribution of frames to the associated ports at both ends of the trunk.
- Trunk links may carry traffic for all VLANs or only specific VLANs.

VLANs and trunking

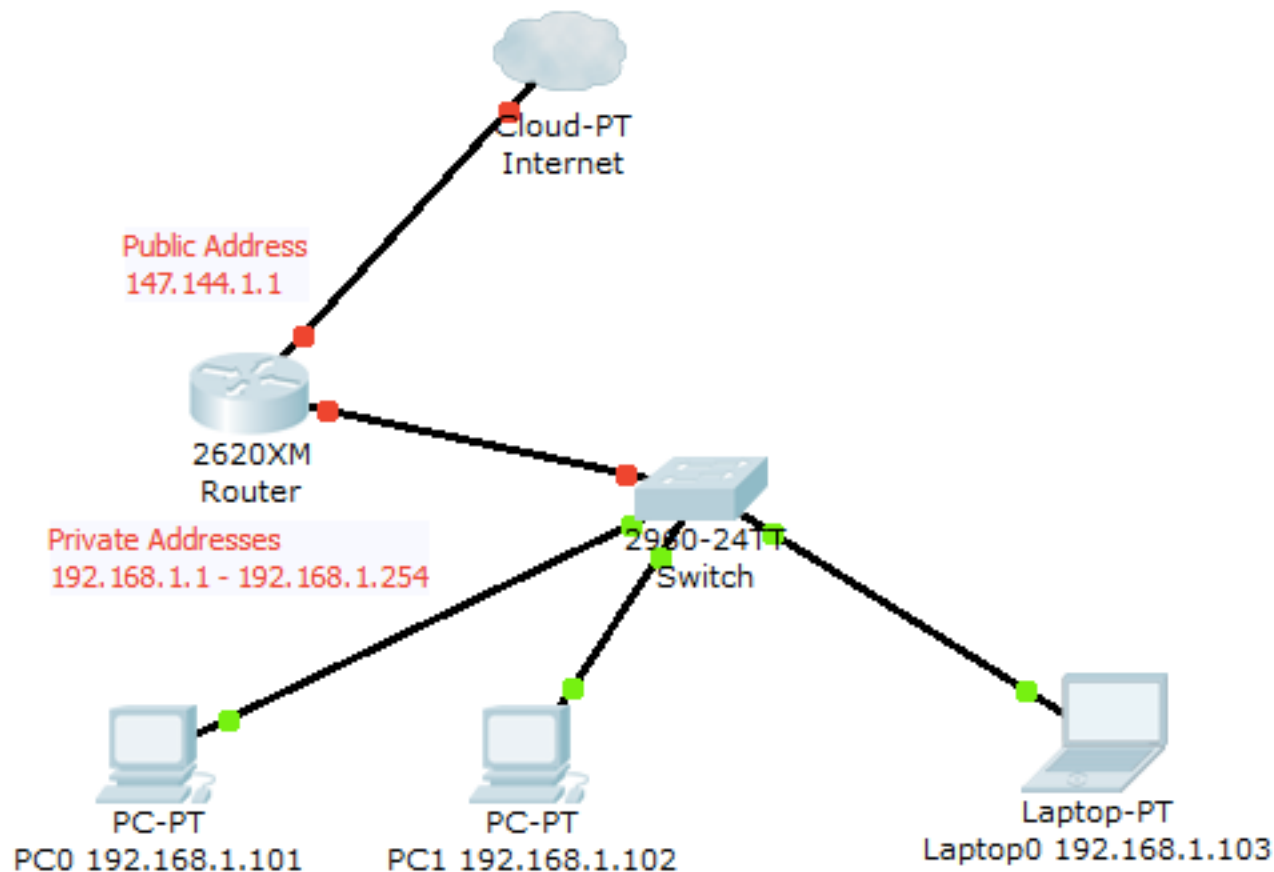


- It is important to understand that a trunk link does not belong to a specific VLAN.
- The responsibility of a trunk link is to act as a conduit for VLANs between switches and routers (or switches and switches).

(Network Address Translation NAT)

- NAT allows many clients to share a single public IP address
- Hides local IP addresses
 - Provides some protection
 - Users can't run unauthorized servers

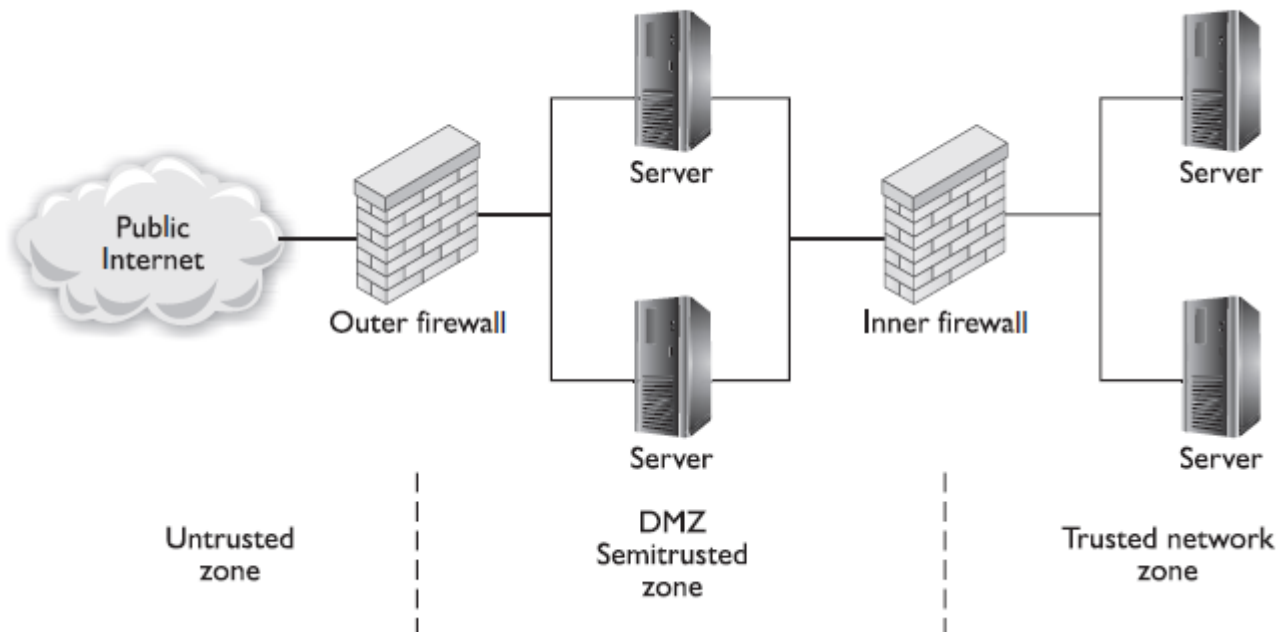
(Network Address Translation NAT)



DMZ (Demilitarized Zone)

- A semi-trusted zone between a private network and the Internet
- Provides *defense in depth* for internal network

CS 07351 – *Cybersecurity: Fundamentals, Principles, and Applications*



Remote Access Protocols

- PPP (Point-to-Point Protocol)
- IPSec (Internet Protocol Security)
- L2TP (Layer 2 Tunneling Protocol)
- RADIUS (Remote Authentication Dial-in User Service)
- TACACS+ (Terminal Access Controller Access-Control System)

But Wait I need to finish

- We talk about IP addresses for Google and others...
- Internet Corporation for Assigned Names and Numbers (ICANN). "is responsible for managing the assignment of network layer addresses (i.e., IP addresses) and application layer addresses (e.g., www.indiana.edu). ICANN sets the rules by which new domain names (e.g., .com, .org, .ca, .uk) are created and IP address numbers.
- For example
- www.google.com is also <http://172.217.8.206/>
- www.amazon.com is also <http://176.32.98.166/>
- www.facebook.com is also <http://31.13.76.102/>
- IP Address Locator <http://ipaddress.com/>

PPP

- Used to create dial-up connections to a server

IPSec

- Can be used as a remote access tunneling protocol
- To encrypt traffic, forming secure connections over the Internet

L2TP

- Combines Microsoft's PPTP with Cisco's L2F
- Often combined with IPSec for encryption
- Port UDP 1701

RADIUS

- Central authentication for remote access clients
- Encrypts passwords only

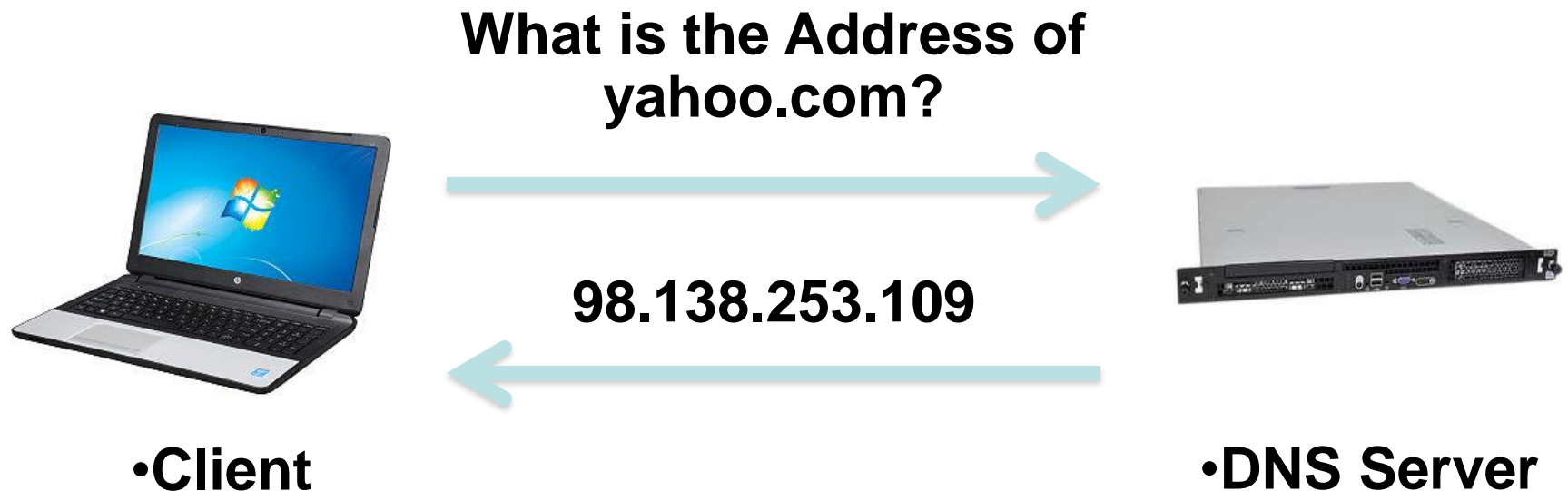
TACACS+

- Used by Cisco VPN concentrators
- Encrypts entire authentication process
- Multiple challenge responses for Authentication, Authorization, and Accounting (AAA)
- Port TCP 49

DNS

- Resolves host names like *www.rowan.edu* into IP addresses like 150.250.205.171
- Ports UDP 53 and TCP 53

Basic DNS Query



- Usually uses UDP port 53
- For large responses, may use TCP port 53

DNS Records

- A IPv4 Address
- AAAA IPv6 Address
- PTR Pointer record
 - Used for reverse DNS lookups
 - Commonly used to block spam email
- MX Mail Exchange
- CNAME Canonical Name
 - Alternate name for a server

SSH

- Used to encrypt Telnet
 - Telnet lacks encryption and uses port TCP 23
- Also used for Secure Copy Protocol (SCP)
- Runs on port TCP 22

SSL

- Can be used to encrypt HTTP traffic, as HTTPS
 - Port TCP 443
- Can also secure LDAP as LDAPS
 - Port TCP 636
- SSL is old and has security weaknesses
 - Demo Self Sign Certificates
 - <http://www.selfsignedcertificate.com/>

TLS

- Replacement for SSL
- Runs on the same ports
 - HTTPS on TCP 443
 - LDAPS on TCP 636

HTTP

- Normal Web browser traffic
- Port TCP 80
- Not encrypted

HTTPS

- Encrypts traffic
- Guarantees identity of server
- Displays padlock in Web browser and HTTPS at start of URL
- Uses SSL or TLS, port TCP 443

FTP

- Upload or download files
- Data in cleartext, including passwords
- Active mode
 - Ports TCP 20 for data and TCP 21 for control
- Passive mode
 - Random port for data and TCP 21 for control

SFTP and FTPS

- SFTP
 - FTP over SSH
 - Port TCP 22
- FTPS
 - FTP over SSL or TLS
 - Ports TCP 989 and 990

Telnet

- Used to send command lines to remote systems
- Uses no encryption, not even for passwords
- Port TCP 23

SNMP

- Used to monitor and manage network devices like routers, switches, and firewalls
- Sends *traps* – signals notifying management systems of their status
- Port UDP 161
- SNMPv1 and v2 sent "community strings" (passwords) in cleartext
- SNMPv3 encrypts passwords

NetBIOS

- Used to resolve Windows computer names like SERVER1 to IP addresses on Local Area Networks
- A legacy protocol, replaced by DNS on most modern networks
- Still used by Windows
- Ports 137-139, both TCP and UDP

LDAP

- Used for directories of users and objects on networks, including
 - Microsoft Active Directory
 - Novell Netware Directory Services
- Port TCP 389 (unencrypted)
- Port TCP 636 (LDAPS, encrypted)

Kerberos

- Uses tickets for authentication
- Used in Windows domains and some Unix environments
- Port 88, both TCP and UDP

SQL Server

- Manages databases
- Often has SSNs, email addresses, account numbers, and other PII (Personally Identifiable Information)
- Commonly hacked via SQL Injection
- Port TCP 1433 (Also UDP 1434)

RDP

- Remotely control a Windows computer
- Service is called "Remote Administration", "Terminal Services", or "Remote Desktop"
- Port TCP 3389
- Also used by Remote Assistance

Email Protocols

- SMTP (Simple Mail Transfer Protocol)
 - Sends mail to other email servers
 - Port TCP 25
- POP3 (Post Office Protocol v3)
 - Moves incoming email to your local Inbox in clients like Outlook
 - Port TCP 110
- IMAP4 (Internet Message Access Protocol v4)
 - Moves incoming email to your local Inbox in clients like Outlook, or lets you view them on the server
 - Port TCP 143

Email Protocols

- Sending a fake email
 - <http://deadfake.com/Send.aspx>
 - <http://www.anonymailer.net/>
 - <http://zmail.sourceforge.net/>
 - <http://www.hongkiat.com/blog/anonymous-email-providers/>

Lab for email

- Mailvelope
- Configure your information
 - Important links
- <https://sks-keyservers.net/>
- <http://pool.sks-keyservers.net:11371/>