Introduction to TCP/IP

Prof. Jong-Moon Chung

Introduction to TCP/IP

- My PC's Internet & Gateway
- TCP/IP Protocol
- Internet Routing & Functions
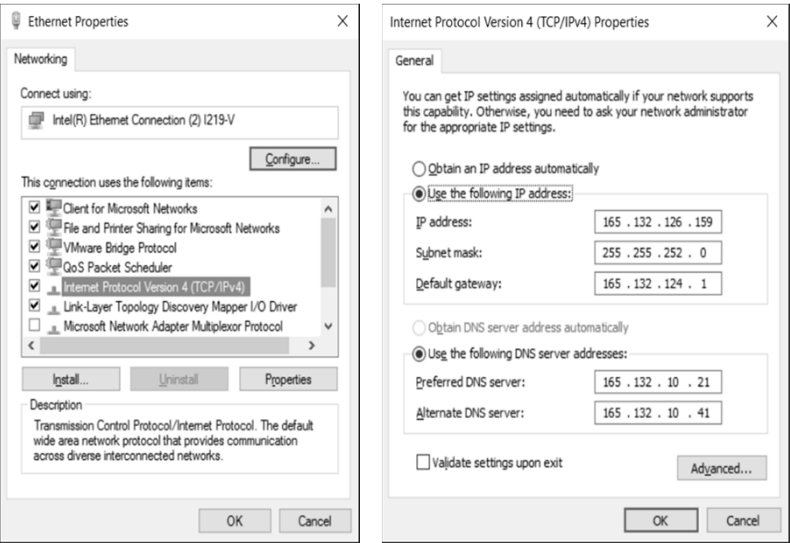- Internet Security
- Wireshark Internet Project

Introduction to TCP/IP

- ## My PC's Internet & Gateway
  - – My PC's Internet Setup
  - – Automatic Internet Setup using DHCP
    (Dynamic Host Configuration Protocol)
  - – IP Gateway/Router Configuration
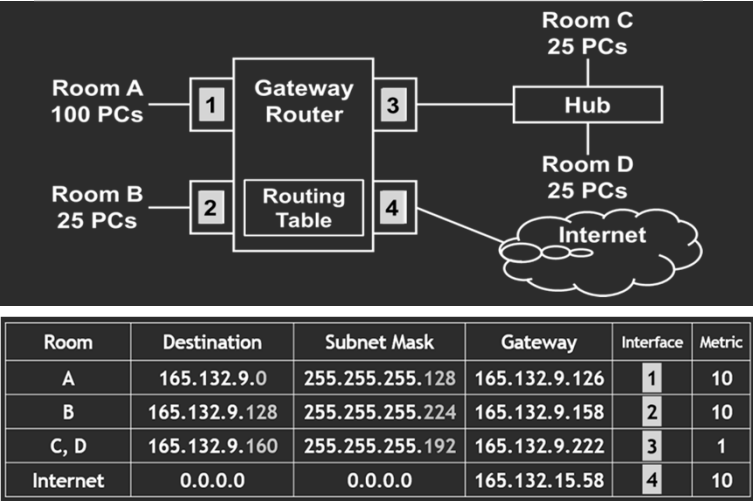 - – IP Routing Table

Introduction to TCP/IP

My PC's Internet & Gateway

Introduction to TCP/IP

My PC's Internet & Gateway

| Room	Destination	Subnet Mask	Gateway	Interface	Metric
A	165.132.9.0	255.255.255.128	165.132.9.126	1	10
B	165.132.9.128	255.255.255.224	165.132.9.158	2	10
C, D	165.132.9.160	255.255.255.192	165.132.9.222	3	1
Internet	0.0.0.0	0.0.0.0	165.132.15.58	4	10

Introduction to TCP/IP

- TCP/IP Protocol
    - OSI vs. TCP/IP
    - TCP/IP Network Operations
    - TCP/IP Layers
    - TCP/IP Networking Functions
    - IPv4 & IPv6
        - CIDR (Classless Inter-Domain Routing)
    - UDP & TCP

Introduction to TCP/IP
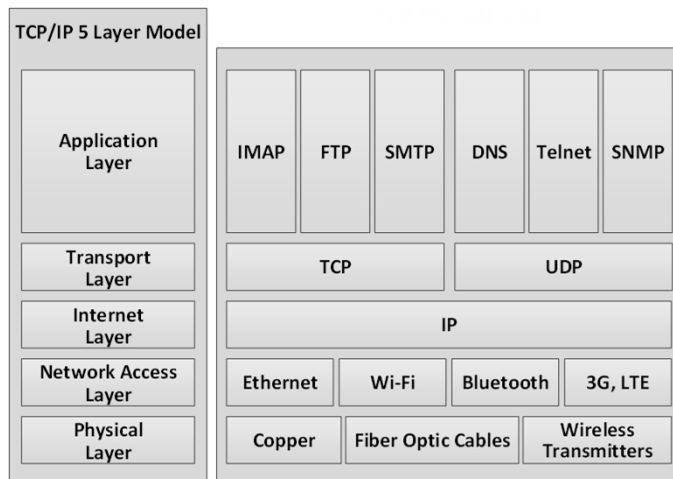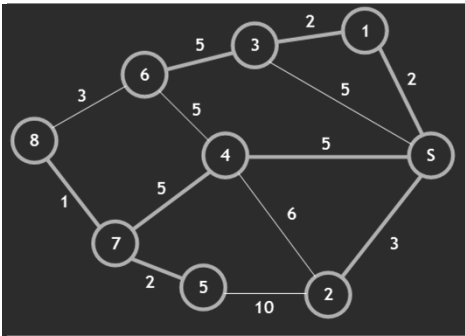
TCP/IP Protocol

Introduction to TCP/IP

- **Internet Routing & Functions**
    - IGP vs. EGP (BGP4)
    - OSPF (Open Shortest Path First) Routing
    - ARP (Address Resolution Protocol)
    - NAT (Network Address Translation)
    - RPC (Remote Procedure Call)
    - FTP (File Transfer Protocol)
    - E-mail (IMAP, POP3, SMTP)

Introduction to TCP/IP

Internet Routing & Functions

OSPF SPT (Shortest Path Tree) Routing

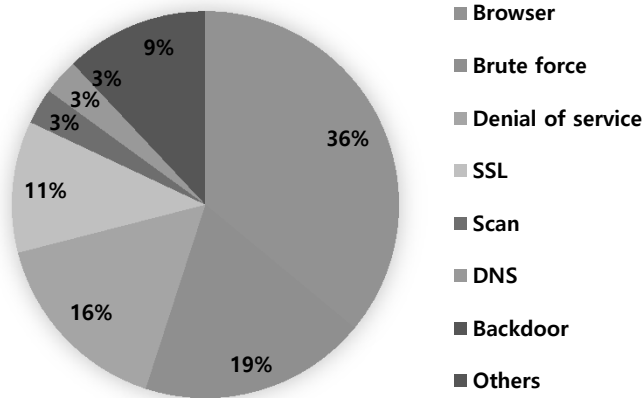| From	To	Route
	1	S → 1
	2	S → 2
	3	S → 1 → 3
	4	S → 4
S	5	S → 4 → 7 → 5
	6	S → 1 → 3 → 6
	7	S → 4 → 7
	8	S → 4 → 7 → 8

Introduction to TCP/IP

- Internet Security
  - Top Ranking Internet Attacks
  - Growing Security & Threat Issues
  - Internet & Cyber Attacks
    - Phishing, DoS, DDoS, Overflow, MITM Attack, SQL Injection
  - Internet Security & Protection
    - Firewall, IDS, TLS, WEP, SSH

Introduction to TCP/IP

Internet Security

Top Ranking Internet Attacks

Legend:
- Browser
- Brute force
- Denial of service
- SSL
- Scan
- DNS
- Backdoor
- Others

Pie chart values: 36%, 19%, 16%, 11%, 3%, 3%, 3%, 9%

2016 McAfee Labs Threat Report, Top 7 network attack types in 2015 Q4

- Calyptix, Top 7 Network Attack Types in 2016, June 13, 2016.
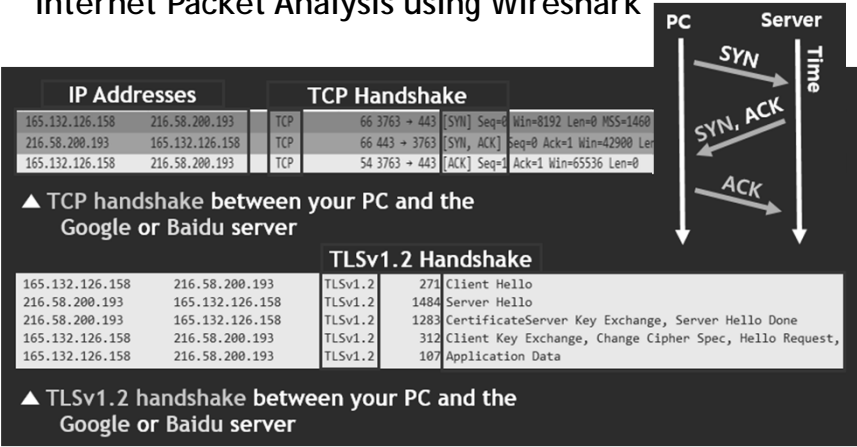- Semantic, 2016 Internet Security Threat Report, vol. 21, April 2016.

Introduction to TCP/IP

- Wireshark Internet Project
  - How to Install Wireshark
  - Internet Packet Analysis using Wireshark

Introduction to TCP/IP

Wireshark Internet Project

Internet Packet Analysis using Wireshark

IP Addresses			TCP Handshake	
165.132.126.158	216.58.200.193	TCP	66 3763 → 443 [SYN] Seq=0	Win=8192 Len=0 MSS=1460
216.58.200.193	165.132.126.158	TCP	66 443 → 3763 [SYN, ACK]	Seq=0 Ack=1 Win=42900 Len
165.132.126.158	216.58.200.193	TCP	54 3763 → 443 [ACK] Seq=1	Ack=1 Win=65536 Len=0

▲ TCP handshake between your PC and the
Google or Baidu server

		TLSv1.2 Handshake		
165.132.126.158	216.58.200.193	TLSv1.2	271	Client Hello
216.58.200.193	165.132.126.158	TLSv1.2	1484	Server Hello
216.58.200.193	165.132.126.158	TLSv1.2	1283	CertificateServer Key Exchange, Server Hello Done
165.132.126.158	216.58.200.193	TLSv1.2	312	Client Key Exchange, Change Cipher Spec, Hello Request,
165.132.126.158	216.58.200.193	TLSv1.2	107	Application Data

▲ TLSv1.2 handshake between your PC and the
Google or Baidu server

Introduction to TCP/IP

- My PC's Internet & Gateway

- TCP/IP Protocol

- Internet Routing & Functions

- Internet Security

- Wireshark Internet Project