Lammle.com

CCNA (200-301) Quick Reference Sheets

NETWORKING FUNDAMENTALS

3 Tier Network Design

- **Access layer:** Provides workgroup/user access to the network; as a result, this layer is sometimes called the workstation layer
- **Distribution layer:** Provides policy-based connectivity and controls the boundary between the access and core layers
- **Core layer:** Provides fast transport between distribution switches within the enterprise campus; this is sometimes called the backbone layer

2 Tier Spine-Leaf Design

This simple 2 tier model is featured in Cisco ACI topologies. It features a spine layer where these core devices connect in a full mesh to every single leaf node.

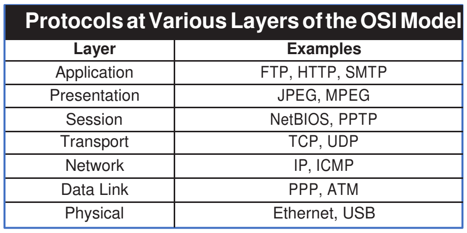
The OSI and TCP/IP Models

OSI model - the layers are:
Application
Presentation
Session
Transport
Network
Data Link
Physical

TCP/IP model - the layers are:
Application
Transport
Internet
Network Interface

The PDUs of the Bottom Four Layers

Segments
Packets
Frames
Bits



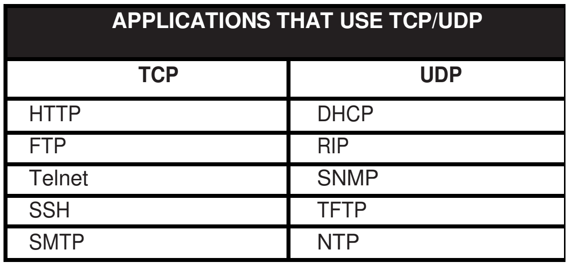
Protocols at Various Layers of the OSI Model

Layer	Examples
Application	FTP, HTTP, SMTP
Presentation	JPEG, MPEG
Session	NetBIOS, PPTP
Transport	TCP, UDP
Network	IP, ICMP
Data Link	PPP, ATM
Physical	Ethernet, USB

TCP vs UDP

UDP is connectionless; UDP has very little overhead; UDP is often used for voice and video traffic forms; UDP can multiplex using port numbers to work with multiple applications.

TCP is connection-oriented; TCP has more overhead than UDP; TCP uses features like flow control, sequencing, and acknowledgements to ensure reliable and ordered delivery of segments; TCP can multiplex using port numbers to work with multiple applications.



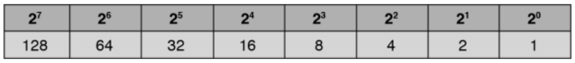
APPLICATIONS THAT USE TCP/UDP

TCP	UDP
HTTP	DHCP
FTP	RIP
Telnet	SNMP
SSH	TFTP
SMTP	NTP

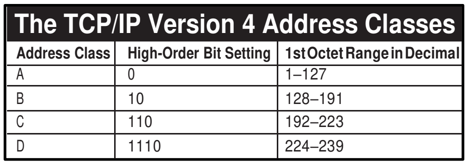
Well-Known Port Number

FTP Data	20	TCP
FTP Control	21	TCP
SSH	22	TCP
Telnet	23	TCP
SMTP	25	TCP
DNS	53	BOTH
DHCP	67, 68	UDP
TFTP	69	UDP
HTTP	80	TCP
POP3	110	TCP
NTP	123	UDP
SNMP	161	UDP
SSL/TLS	443	TCP
Syslog	514	UDP
RIP	520	UDP

A Conversion Chart for IPv4 Addressing and Subnetting Questions

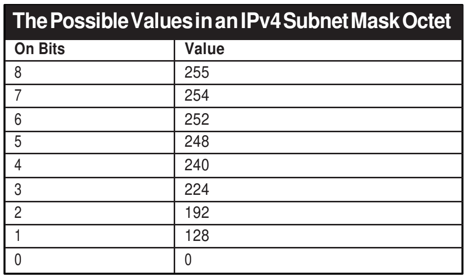


2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1



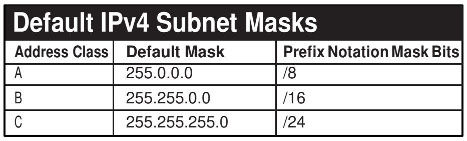
The TCP/IP Version 4 Address Classes

Address Class	High-Order Bit Setting	1st Octet Range in Decimal
A	0	1–127
B	10	128–191
C	110	192–223
D	1110	224–239



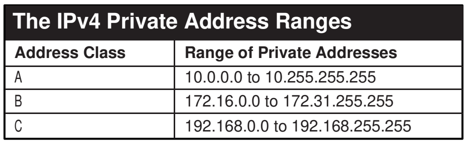
The Possible Values in an IPv4 Subnet Mask Octet

On Bits	Value
8	255
7	254
6	252
5	248
4	240
3	224
2	192
1	128
0	0



Default IPv4 Subnet Masks

Address Class	Default Mask	Prefix Notation Mask Bits
A	255.0.0.0	/8
B	255.255.0.0	/16
C	255.255.255.0	/24



The IPv4 Private Address Ranges

Address Class	Range of Private Addresses
A	10.0.0.0 to 10.255.255.255
B	172.16.0.0 to 172.31.255.255
C	192.168.0.0 to 192.168.255.255

Modified EUI-64 Host Portion Assignment

```
interface gi0/0
ipv6 address 2001:AAAA:BBBB::/64 eui-64
```

Using SLAAC for Address Assignment on a Cisco Router

```
interface gi0/0
ipv6 address autoconfig
```

NETWORK ACCESS

Creating a VLAN on a Cisco Switch

```
configure terminal
vlan 30
name 1STFLOOREAST
```

Configuring an Interface for VLAN (Access Port)

```
interface gi0/2
switchport mode access
switchport access vlan 30
```

Configuring Trunking

```
interface gi0/10
switchport trunk encapsulation dot1q
switchport mode trunk
```

Wireless Technologies

RF Bands: There are two main radio frequency bands used with WiFi technologies. The 2.4 GHz band and the 5 GHz band. For example, 802.11g uses the 2.4 GHz band, while 802.11ac uses the 5 GHz band.

SSID: This is the “friendly” name of the wireless network.

Non-overlapping channels: Channels 1, 6, 11 are non-overlapping channels that permit you to configure wireless LANs that function properly.

Wireless LAN Controller (WLC): The WLC is a device for configuring, monitoring, and troubleshooting the wireless LAN. For example, wireless Access Points can be “lightweight” and can rely on WLCs for the “intelligence” required to form the WLAN.

IP CONNECTIVITY

Default Admin Distances (Cisco)

Connected	0
Static	1
EIGRP summary	5
EBGP	20
Internal EIGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
External EIGRP	170
IBGP	200
Unknown	255

Configuring a Default Static Route

```
configure terminal
ip route 0.0.0.0 0.0.0.0 10.10.10.2
```

Configuring an IPv6 Static Route

```
configure terminal
ipv6 route 2001:aaa::/64 serial0/0
```

Configuring a Floating Static Route

```
configure terminal
ip route 10.0.0.0 255.0.0.0 10.0.0.1 121
```

A Sample OSPF Configuration (Network Command)

```
configure terminal
router ospf 1
network 10.0.0.0 0.255.255.255 area 0
```

A Sample OSPF Configuration (Interface Level)

```
configure terminal
interface gi0/0
ip ospf 1 area 0
```

IP SERVICES

Inside Source Dynamic PAT

```
configure terminal
access-list 1 permit 192.168.1.0 0.0.0.255
ip nat inside source list 1 interface gi0/0
overload
interface gi0/1
ip nat inside
interface gi0/0
ip nat outside
```

DHCP Server on Cisco Router

```
configure terminal
ip dhcp excluded-address 10.1.1.1 10.1.1.10
ip dhcp pool CCNAPOOL
network 10.1.1.0/24
default-router 10.1.1.1
dns-server 8.8.8.8
option 150 ip 10.1.1.2
```

Configuring a DHCP Relay Agent

```
configure terminal
interface gi0/0
ip helper-address 10.1.1.1
```

Configuring the NTP Server

```
configure terminal
ntp master 3
```

Configuring the NTP Client

```
ntp server 10.1.1.1
```

SECURITY FUNDAMENTALS

Wireless LAN Security

WEP: WEP is no longer considered acceptable as a security solution. This technique is “hacked” with relative ease.

WPA: WPA was the first attempt at replacing WEP. There were some security issues discovered with this technology that gave rise (quickly) to WPA2.

WPA2: WPA2 is considered strong enough for use today. It replaced TKIP (which had weaknesses) with CCMP. Like WPA, it uses AES for encryption. TKIP is still present in the protocol, but only for backward compatibility with WPA.

WPA3: Like WPA2, this latest version of the security protocol permits you to configure a "personal" or home version, compared to a stronger "enterprise" version.

Common Cybersecurity Threats

Computer Viruses
Malware
Trojans
Adware and spyware
Worms
DDoS
Phishing
Rootkit
SQL injection attack
Main-in-the-middle
Ransomware
Data exfiltration

Configuring an Extended ACL

```
ip access-list extended MYACL
deny tcp 192.168.8.0 0.0.0.255 any eq 443
permit ip any any
```

Configuring Static Port Security

```
interface gi0/10
switchport mode access
switchport port-security maximum 2
switchport port-security mac-address
f116.3e20.58f1
switchport port-security mac-address
f116.32e1.45a1
```

AUTOMATION AND PROGRAMMABILITY

Controller-based networking: Software defined networking (SDN) often features the use of a central controller that implements the control plane functions required by the network. The devices that are controlled in SDN can focus on the forwarding of traffic. The SDN approach fosters efficient, automated, highly controlled networks.

REST APIs: These APIs are often used for cloud and SDN technologies. They ensure that you can retrieve data using "standard" URLs understood by web browsers and Internet technologies.

JSON: This is a very friendly way to represent data in a human readable form. JSON presents data as a series of attribute-value pairs. It is very similar to XML, but even more easily readable by us humans.

Puppet, Chef, and Ansible: These tools allow you to easily manage network devices from a central location. The tools use different techniques. For example, Puppet uses an agent on the various network devices, while Ansible is often celebrated as it is agent-less.

CRUD:

Create
Read
Update
Delete