CSF 432: Intro to Network and System Security

Week 03 - Review

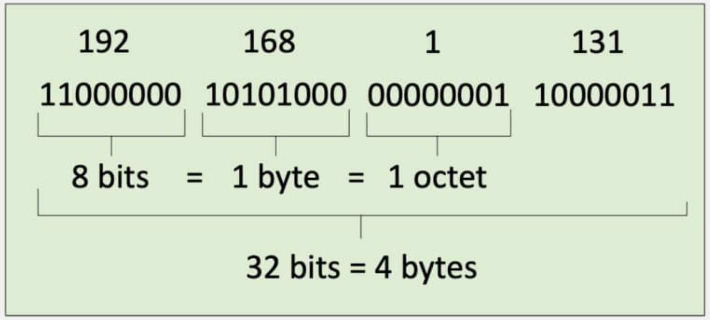
Michael Conti

Department of Computer Science and Statistics
University of Rhode Island

Fall 2020

Sources: Professor Messer's CompTIA N10-007 Network+ Course Notes

IPv4 and IPv6 Addressing



192	168	1	131
11000000	10101000	00000001	10000011

8 bits = 1 byte = 1 octet

32 bits = 4 bytes

IPv4 and IPv6 Addressing

The IP address of a device

- ☑ IP Address, e.g., 192.168.1.165
  - ☑ Every device needs a unique IP address
- ☑ Subnet mask, e.g., 255.255.255.0
  - ☑ Used by the local workstation to determine what subnet it's on
  - ☑ The subnet mask isn't (usually) transmitted across the network
- ☑ You'll ask for the subnet mask all the time
  - ☑ What's the subnet mask of this network?

IPv4 and IPv6 Addressing

The secret behind the IP address

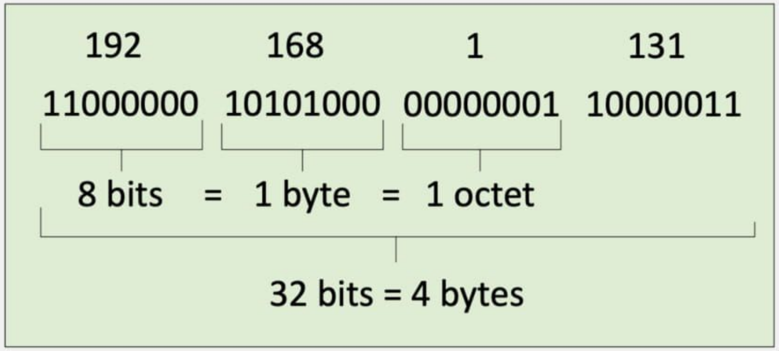
- ☑ The IP address isn't really a single address.
- ☑ An IP address is a combination of a network ID and a host ID
  - ☑ The subnet mask determines what part of the IP address is the network and which part is the host
  - ☑ The subnet mask is just as important as your IP address!
- ☑ The best way to see this work is in binary
  - ☑ This is the (very easy) math part

IPv4 and IPv6 Addressing

IPv4 addresses - Internet Protocol version 4

☑ OSI Layer 3 address

☑ Since one byte is 8 bits, the maximum decimal value for each byte is 255



192 168 1 131

11000000 10101000 00000001 10000011

8 bits = 1 byte = 1 octet

32 bits = 4 bytes

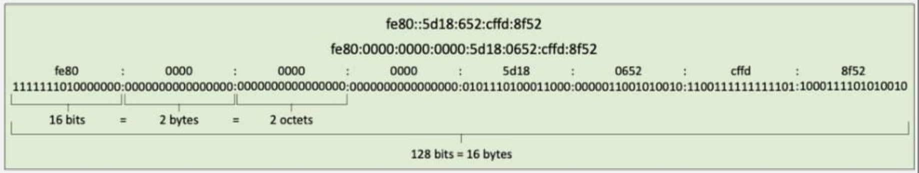
IPv4 and IPv6 Addressing

IPv6 addresses

☑ Internet Protocol v6 - 128-bit address

☑ 340,282,366,920,938,463,463,374,607,431,768,211,456 addresses (340 undecillion)

☑ 6.8 billion people could have 5,000,000,000,000,000,000,000,000,000 addresses each



fe80::5d18:652:cffd:8f52

fe80:0000:0000:0000:5d18:0652:cffd:8f52

```
fe80 : 0000 : 0000 : 0000 : 5d18 : 0652 : cffd : 8f52
1111111010000000:0000000000000000:0000000000000000:0000000000000000:0101110100011000:0000011001010010:1100111111111101:1000111101010010
```

16 bits = 2 bytes = 2 octets

128 bits = 16 bytes

IPv4 and IPv6 Addressing

IPv6 address compression

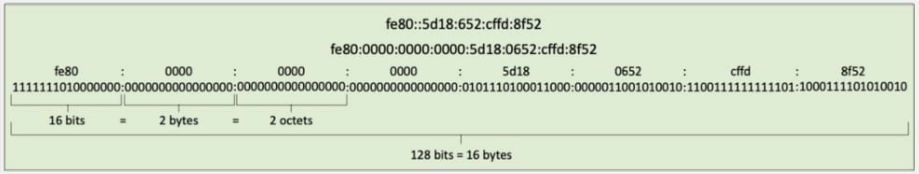
☑ Your DNS will become very important!

☑ Groups of zeros can be abbreviated with a double colon ::

- ☑ Only one of these abbreviations allowed per address

☑ Leading zeros are optional

Configuring IPv6



fe80::5d18:652:cffd:8f52

fe80:0000:0000:0000:5d18:0652:cffd:8f52

```
fe80 : 0000 : 0000 : 0000 : 5d18 : 0652 : cffd : 8f52
1111111010000000:0000000000000000:0000000000000000:0000000000000000:0101110100011000:0000011001010010:1100111111111101:1000111101010010
```

16 bits = 2 bytes = 2 octets

128 bits = 16 bytes

Configuring IPv6

Dual-stack routing

- ☑ Dual-stack IPv4 and IPv6
  - ☑ Run both at the same time
  - ☑ Interfaces will be assigned multiple address types
- ☑ IPv4
  - ☑ Configured with IPv4 addresses
  - ☑ Maintains an IPv4 routing table
  - ☑ Uses IPv4 dynamic routing protocols
- ☑ IPv6
  - ☑ Configured with IPv6 addresses
  - ☑ Maintains a separate IPv6 routing table
  - ☑ Uses IPv6 dynamic routing protocols

Configuring IPv6

Tunneling IPv6

- ☑ 6 to4 addressing
  - ☑ Send IPv6 over an existing IPv4 network
  - ☑ Creates an IPv6 based on the IPv4 address
  - ☑ Requires relay routers -
    - □ IP protocol 41 - a transition technology
- ☑ No support for NAT
- ☑ 4in6
  - ☑ Tunnel IPv4 traffic on an IPv6 network

Configuring IPv6

Teredo/Miredo

- ☑ Tunnel IPv6 through NATed IPv4
  - ☑ End-to-end IPv6 through an IPv4 network
  - ☑ No special IPv6 router needed
    - □ Temporary use
  - ☑ We'll have IPv6 native networks soon (?)
- ☑ Miredo - Open-source Teredo for Linux,
- ☑ BSD Unix, and Mac OS X
  - ☑ Full functionality

Configuring IPv6

NDP (Neighbor Discovery Protocol)

- ☑ No broadcasts!
  - ☑ Operates using multicast over ICMPv6
- ☑ Neighbor MAC Discovery
  - ☑ Replaces the IPv4 ARP
- ☑ SLAAC (Stateless Address Autoconfiguration)
  - ☑ Automatically configure an IP address without a DHCP server
- ☑ DAD (Duplicate Address Detection)
  - ☑ No duplicate IPs!
- ☑ Discover routers
  - ☑ Router Solicitation (RS) and Router Advertisement (RA)

Configuring IPv6

Finding Router

- ICMPv6 adds the Neighbor Discovery Protocol
- Routers also send unsolicited RA messages
  - From the multicast destination of ff02::1
- Transfers IPv6 address information, prefix value, and prefix length, etc.
  - Sent as a multicast
- Neighbor Advertisement (NA)

Configuring IPv6

Howdy Neighbor

- There’s no ARP in IPv6
  - So how do you find out the MAC address of a device?
- Neighbor Solicitation (NS)
  - Sent as a multicast
- Neighbor Advertisement (NA)

Prioritizing Traffic

Prioritizing Traffic

Managing Network Traffic

- Many different devices
  - Desktop, laptop, VoIP phone, mobile devices
- Many different applications
  - Mission critical applications, streaming video, streaming audio
- Different apps have different network requirements
  - Voice is real-time
  - Recorded streaming video has a buffer
  - Database application is interactive
- Some applications are “more important” than others
  - Voice traffic needs to have priority over YouTube

Prioritizing Traffic

Packet shaping

☑ Packet shaping, traffic shaping

☑ Control by bandwidth usage or data rates

☑ Set important applications to have higher priorities than other apps

QoS (Quality of Service)

☑ Prioritize traffic performance

- ☑ Voice over IP traffic has priority over web-browsing
- ☑ Prioritize by maximum bandwidth, traffic rate, VLAN, etc.

☑ Quality of Service

- ☑ Describes the process of controlling traffic flows

☑ Many different methods - Across many different topologies

Prioritizing Traffic

Managing QoS

☑ CoS (Class of Service)

- ☑ OSI Layer 2
- ☑ Ethernet frame header in an 802.1q trunk
- ☑ Usually applied in the intranet (not from an ISP)

☑ Differentiated Services (DiffServ)

- ☑ OSI Layer 3
- ☑ QoS bits are enabled in the IPv4 header
- ☑ Bits are set external to the application
- ☑ Routers and switches have to play along

☑ DSCP (Differentiated Services Code Point)

- ☑ DS (Differentiated Services) field in the IP header

Network Address Translation (NAT)

IP address range	Number of addresses	Classful description	Largest CIDR block (subnet mask)	Host ID size
10.0.0.0 – 10.255.255.255	16,777,216	single class A	10.0.0.0/8 (255.0.0.0)	24 bits
172.16.0.0 – 172.31.255.255	1,048,576	16 contiguous class Bs	172.16.0.0/12 (255.240.0.0)	20 bits
192.168.0.0 – 192.168.255.255	65,536	256 contiguous class Cs	192.168.0.0/16 (255.255.0.0)	16 bits

Network Address Translation (NAT)

NAT (Network Address Translation)

☑ It is estimated that there are over 20 billion devices connected to the Internet (and growing)

- ☑ IPv4 supports around 4.29 billion addresses

☑ The address space for IPv4 is exhausted

- ☑ There are no available addresses to assign

☑ How does it all work?

- ☑ Network Address Translation

☑ This isn't the only use of NAT

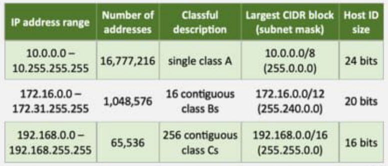
- ☑ NAT is handy in many situations

IP address range	Number of addresses	Classful description	Largest CIDR block (subnet mask)	Host ID size
10.0.0.0 – 10.255.255.255	16,777,216	single class A	10.0.0.0/8 (255.0.0.0)	24 bits
172.16.0.0 – 172.31.255.255	1,048,576	16 contiguous class Bs	172.16.0.0/12 (255.240.0.0)	20 bits
192.168.0.0 – 192.168.255.255	65,536	256 contiguous class Cs	192.168.0.0/16 (255.255.0.0)	16 bits

Network Address Translation (NAT)

Port Forwarding

- 24x7 access to a service hosted internally
  - Web server, gaming server, security system, etc.
- External IP/port number maps to an internal IP/port
  - Does not have to be the same port number
- Also called Destination NAT or Static NAT
  - Destination address is translated from a public IP to a private IP
  - Does not expire or timeout



IP address range	Number of addresses	Classful description	Largest CIDR block (subnet mask)	Host ID size
10.0.0.0 – 10.255.255.255	16,777,216	single class A	10.0.0.0/8 (255.0.0.0)	24 bits
172.16.0.0 – 172.31.255.255	1,048,576	16 contiguous class Bs	172.16.0.0/12 (255.240.0.0)	20 bits
192.168.0.0 – 192.168.255.255	65,536	256 contiguous class Cs	192.168.0.0/16 (255.255.0.0)	16 bits

Access Control Lists

Access Control Lists

Packet filtering

- Used to allow or deny traffic
  - Also used for NAT, QoS, etc.
- Defined on the ingress or egress of an interface
  - Incoming or outgoing
- ACLs can evaluate on certain criteria
  - Source IP, Destination IP, TCP port numbers, UDP port numbers, ICMP
- Deny or permit
  - What happens when an ACL matches the traffic?
- ACLs have evolved through the years
  - More options and features available for traffic filtering

Access Control Lists

Firewall rules

- Access control lists (ACLs)
  - Allow or disallow traffic based on tuples
  - Groupings of categories
    - Source IP, Destination IP, port number, time of day, application, etc.
- A logical path
  - Usually top-to-bottom
- Can be very general or very specific
  - Specific rules are usually at the top
- Implicit deny
  - Most firewalls include a deny at the bottom
    - Even if you didn't put one

Circuit Switching and Packet Switching

Circuit Switching and Packet Switching

Circuit switching

- ☑ Circuit is established between endpoints before data passes
  - ☑ Like a phone call
- ☑ Nobody else can use the circuit when it's idle
  - ☑ Inefficient use of resources
- ☑ Connection is always there
  - ☑ It's mine. You can't use it.
- ☑ Capacity is guaranteed
  - ☑ You'd better use it, you paid for it.
- ☑ POTS (plain old telephone service) and PSTN (public switched telephone network)
- ☑ T1 / E1 / T3 / E3
  - ☑ Create a circuit between two sites
- ☑ ISDN
  - ☑ Use a phone number to call another ISDN modem

Circuit Switching and Packet Switching

Packet switching

- ☑ Data is grouped into packets
  - ☑ Voice, data, video, etc.
  - ☑ Like a network
- ☑ The media is usually shared
  - ☑ Someone else can use it, even when you don't
- ☑ One connection may have more bandwidth allocated than another
  - ☑ How much money would you like to spend?
- ☑ SONET, ATM
- ☑ DSL
- ☑ Frame relay
- ☑ MPLS
- ☑ Cable modem
- ☑ Satellite
- ☑ Wireless

Software Defined Networking

Software Defined Networking

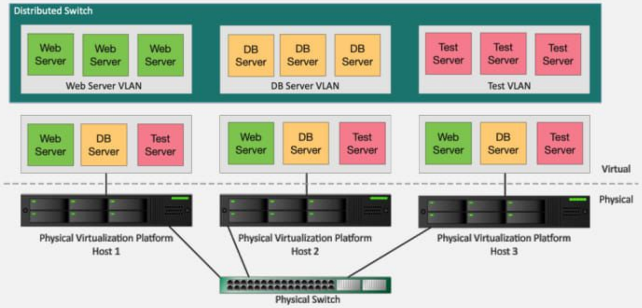
SDN (Software Defined Networking)

- ☑ Networking devices have two functional planes of operation
  - ☑ Control plane
  - ☑ Data plane
- ☑ Directly programmable
  - ☑ Configuration is different than forwarding
- ☑ Agile
  - ☑ Changes can be made dynamically
- ☑ Centrally managed - Global view, single pane of glass
- ☑ Programmatically configured
  - ☑ Orchestration - No human intervention
- ☑ Open standards / vendor neutral
  - ☑ A standard interface to the network

Software Defined Networking

Distributed switching

- ☑ Remove the physical segmentation
  - ☑ A virtual network distributed across all physical platforms
- ☑ When a VM moves, the network doesn't change
  - ☑ Servers will always connect to the right VLAN



CSF 432: Intro to Network and System Security

Week 03 - Review

Michael Conti

Department of Computer Science and Statistics
University of Rhode Island

Fall 2020

Sources: Professor Messer's CompTIA N10-007 Network+ Course Notes