CSF 432: Intro to Network and System Security

Week 05 - Review

Michael Conti

Department of Computer Science and Statistics
University of Rhode Island

Fall 2020

Assigning IPv4 Addresses

Assigning IPv4 Addresses

DHCP

☑ IPv4 address configuration used to be manual

　☑ IP address, subnet mask, gateway, DNS servers, NTP servers, etc.

☑ October 1993 - The bootstrap protocol - BOOTP

☑ BOOTP didn't automatically define everything

　☑ Some manual configurations were still required

　☑ BOOTP also didn't know when an IP address might be available again

☑ Dynamic Host Configuration Protocol

　☑ Initially released in 1997, updated through the years

　☑ Provides automatic address / IP configuration for almost all devices

---

Assigning IPv4 Addresses

The DHCP Process

☑ Step 1: Discover - Client to DHCP Server

　☑ Find all of the available DHCP Servers

☑ Step 2: Offer - DHCP Server to client

　☑ Send some IP address options to the client

☑ Step 3: Request - Client to DHCP Server

　☑ Client chooses an offer and makes a formal request

☑ Step 4: Acknowledgement - DHCP Server to client
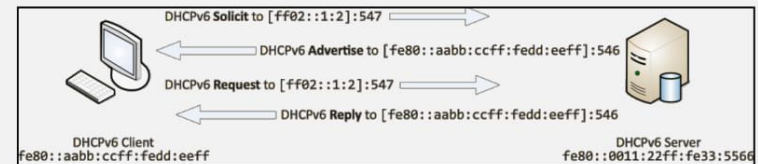
　☑ DHCP server sends an acknowledgement to the client

Assigning IPv4 Addresses

Turning dynamic into static

☑ DHCP assigns an IP address from the first available from a large pool of addresses

  ☑ Your IP address will occasionally change

☑ You may not want your IP address to change

  ☑ Server, printer, or personal preference

☑ Disable DHCP on the device

  ☑ Configure the IP address information manually

  ☑ Requires additional administration

☑ Configure an IP reservation on the DHCP server

  ☑ Associate a specific MAC address with an IP address
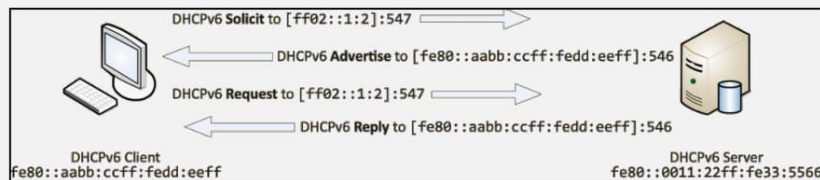

Assigning IPv6 Addresses

DHCPv6 Solicit to [ff02::1:2]:547
DHCPv6 Advertise to [fe80::aabb:ccff:fedd:eeff]:546
DHCPv6 Request to [ff02::1:2]:547
DHCPv6 Reply to [fe80::aabb:ccff:fedd:eeff]:546

DHCPv6 Client
fe80::aabb:ccff:fedd:eeff

DHCPv6 Server
fe80::0011:22ff:fe33:5566

Assigning IPv6 Addresses

Stateful DHCPv6

☑ Very similar process to DHCPv4 - udp/546 (client) and udp/547 (server)

DHCPv6 Solicit to [ff02::1:2]:547
DHCPv6 Advertise to [fe80::aabb:ccff:fedd:eeff]:546
DHCPv6 Request to [ff02::1:2]:547
DHCPv6 Reply to [fe80::aabb:ccff:fedd:eeff]:546

DHCPv6 Client
fe80::aabb:ccff:fedd:eeff

DHCPv6 Server
fe80::0011:22ff:fe33:5566

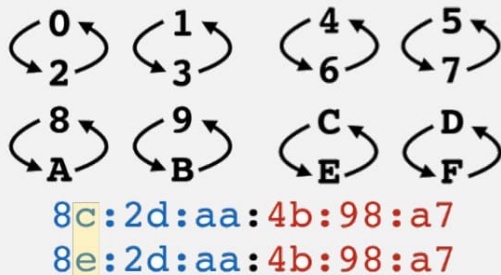## Assigning IPv6 Addresses

Converting EUI-48 to EUI-64

☑ Split the MAC

  ☑ Two 3-byte (24 bit) halves

☑ Put FFFE in the middle

  ☑ The missing 16 bits

☑ Invert the seventh bit

  ☑ Changes the address from globally unique/universal

  ☑ Turns the burned-in address (BIA) into a locally administered address

  ☑ This is the U/L bit (universal/local)
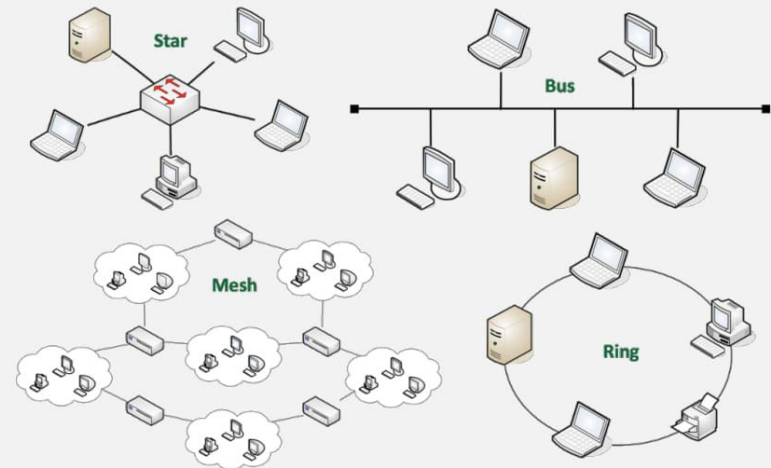
Slide 9

Assigning IPv6 Addresses

Shortcut for flipping the 7th bit

☑ Quickly convert the MAC address - create a chart

☑ Count from 0 to F in hex - two columns, groups of four

☑ Quickly convert the second character of the first hex byte

  ☑ Change it to the other value

0 ↔ 2   1 ↔ 3   4 ↔ 6   5 ↔ 7

8 ↔ A   9 ↔ B   C ↔ E   D ↔ F

8c:2d:aa:4b:98:a7
8e:2d:aa:4b:98:a7

Slide 10

Network Topologies

Star

Bus

Mesh

Ring

Slide 11

Network Topologies

Logical Network Maps

☑ Specialized software

  ☑ Visio, OmniGraffle, Gliffy.com

☑ High level views

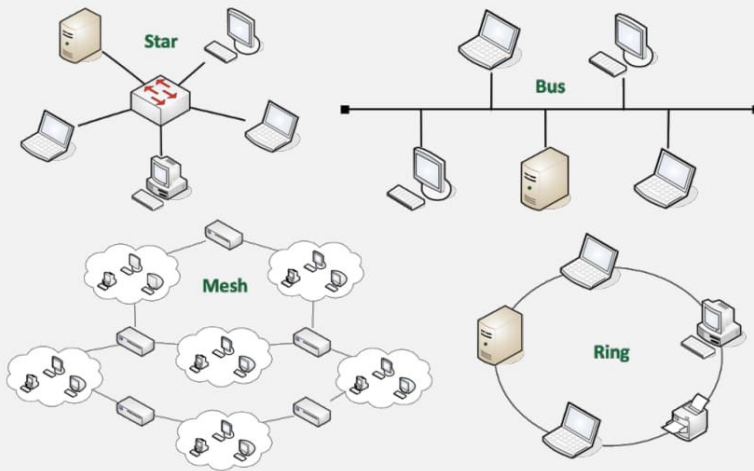 ☑ WAN layout, application flows

☑ Useful for planning and collaboration

Physical network maps

☑ Follows the physical wire and device

  ☑ Can include physical rack locations

Slide 12

Common Network Types

Network Topologies

Wireless topologies

☑ Ad hoc networking

- ☑ No pre-existing infrastructure
- ☑ Devices communication amongst themselves

☑ Infrastructure

- ☑ All devices communicate through an access point
- ☑ The most common wireless communication mode

☑ Mesh

- ☑ Ad hoc devices work together to form a mesh "cloud"
- ☑ Self form and self heal

Common Network Types

LAN - Local Area Network

☑ A building or group of buildings

- ☑ High-speed connectivity

☑ Ethernet and 802.11 wireless

- ☑ Any slower and it isn't "local"

WLAN - Wireless LAN

☑ 802.11 technologies

☑ Mobility within a building or geographic area

☑ Expand coverage with additional access points MAN - Metropolitan Area

Common Network Types

MAN - Metropolitan Area Network

☑ A network in your city

- ☑ Larger than a LAN, often smaller than a WAN

☑ Common to see government ownership

- ☑ They "own" the right-of-way

CAN - Campus Area Network

☑ Corporate Area Network

☑ Limited geographical area

- ☑ A group of buildings

☑ LAN technologies

- ☑ Fiber connected, high speed Ethernet

☑ Your fiber in the ground

- ☑ No third-party provider

Common Network Types

WAN - Wide Area Network

☑ Generally connects LANs across a distance

☑ And generally much slower than the LAN

☑ Many different WAN technologies

☑ Point-to-point serial, MPLS, et

☑ Terrestrial and non-terrestrial

Common Network Types

NAS vs. SAN

☑ **Network Attached Storage (NAS)**

☑ Connect to a shared storage device across the network

☑ File-level access

☑ **Storage Area Network (SAN)**

☑ Looks and feels like a local storage device

☑ Block-level access

☑ Very efficient reading and writing

☑ Requires a lot of bandwidth

☑ May use an isolated network and high-speed network technologies

Common Network Types

PAN - Personal Area Network

☑ Personal Area Network

☑ Your own private network - Bluetooth, IR, NFC

☑ Automobile - audio output, integrate with phone

☑ Mobile phone - wireless headset

☑ Health - workout telemetry, daily reports

Internet of Things (IoT) Topologies

Internet of Things (IoT) Topologies

Internet of Things

☑ Wearable technology

☑ Watches, health monitors, glasses

☑ Track our location

☑ Where is that data and how is it stored?

☑ Home automation

☑ Video doorbells

☑ Internet-connected garage door openers

☑ Heating and cooling

☑ It knows when you are home (and when you aren't)

Internet of Things (IoT) Topologies

Z-Wave

☑ Home automation networking

☑ Control lights, locks, garage doors, etc.

☑ Wireless mesh networking

☑ Nodes can hop through other nodes on the way to the destination

☑ Uses the ISM band

☑ Industrial, Scientific, and Medical

☑ 900 MHz frequencies in the US

☑ No conflicts with 802.11

Internet of Things (IoT) Topologies

ANT / ANT+

☑ Wireless sensor network protocol

☑ 2.4 GHz ISM band (industrial, scientific, and medical)

☑ An "Internet of Things" ultra-low-power protocol

☑ Fitness devices, heart rate monitors, etc.

☑ A separate wireless service

☑ Not 802.11 or Bluetooth

☑ Denial of service

☑ Spectrum jamming

☑ Optional encryption

☑ And no method to maintain integrity

Internet of Things (IoT) Topologies

Bluetooth

☑ High speed communication over short distances

☑ PAN (Personal Area Network)

☑ Connects our mobile devices

☑ Smartphones, tethering, headsets and headphones,

☑ health monitors, automobile and phone integration, smartwatches, external speakers

Internet of Things (IoT) Topologies

Near field communication (NFC)

☑ Two-way wireless communication

  ☑ Builds on RFID, which is mostly one-way

☑ Payment systems

  ☑ Google wallet and MasterCard partnership

☑ Bootstrap for other wireless

  ☑ NFC helps with Bluetooth pairing

☑ Access token, identity "card"

  ☑ Short range with encryption support

Internet of Things (IoT) Topologies

RFID (Radio-frequency identification)

☑ It's everywhere

  ☑ Access badges

  ☑ Inventory/Assembly line tracking

  ☑ Pet/Animal identification

  ☑ Anything that needs to be tracked

☑ Radar technology

  ☑ Radio energy transmitted to the tag

  ☑ RF powers the tag, ID is transmitted back

  ☑ Bidirectional communication

  ☑ Some tag formats can be active/powered

Internet of Things (IoT) Topologies

IR (Infrared)

☑ Included on many smartphones, tablets, and smartwatches

  ☑ Not really used for file transfers and printing

☑ Control your entertainment center

  ☑ Many IR options

IEEE 802.11

☑ Wireless networking (802.11)

  ☑ Managed by the IEEE LAN/MAN Standards Committee (IEEE 802)

☑ Many updates over time

  ☑ Check with IEEE for the latest

☑ The Wi-Fi trademark

  ☑ Wi-Fi Alliance handles interoperability testing

Wireless Standards

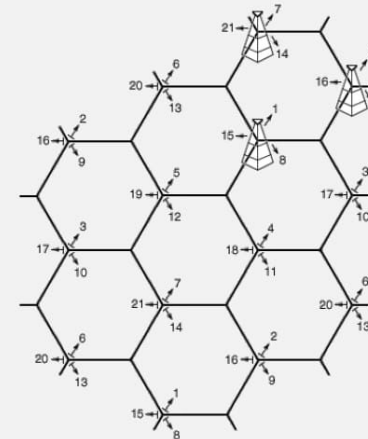|	Frequencies	Maximum MIMO streams	theoretical throughput (per stream)	theoretical throughput (total)
802.11a	5 GHz	Not applicable	54 Mbit/s	54 Mbit/s
802.11b	2.4 GHz	Not applicable	11 Mbit/s	11 Mbit/s
802.11g	2.4 GHz	Not applicable	54 Mbit/s	54 Mbit/s
802.11n	5 GHz and/or 2.4 GHz	4 MIMO	150 Mbit/s	600 Mbit/s
802.11ac	5 GHz	8 MU-MIMO	866.7 Mbit/s	~6.8 Gbit/s

Wireless Standards

☑ 802.11a ☑ 802.11n

☑ 802.11b ☑ 802.11ac

☑ 802.11g

|	Frequencies	Maximum MIMO streams	theoretical throughput (per stream)	theoretical throughput (total)
802.11a	5 GHz	Not applicable	54 Mbit/s	54 Mbit/s
802.11b	2.4 GHz	Not applicable	11 Mbit/s	11 Mbit/s
802.11g	2.4 GHz	Not applicable	54 Mbit/s	54 Mbit/s
802.11n	5 GHz and/or 2.4 GHz	4 MIMO	150 Mbit/s	600 Mbit/s
802.11ac	5 GHz	8 MU-MIMO	866.7 Mbit/s	~6.8 Gbit/s

Cellular Network Standards

Cellular Network Standards

Cellular networks

☑ Mobile devices - "Cell" phones

☑ Separate land into "cells"

　☑ Antenna coverages a cell with certain frequencies

☑ 2G networks

　☑ GSM - Global System for Mobile Communications

　☑ CDMA - Code Division
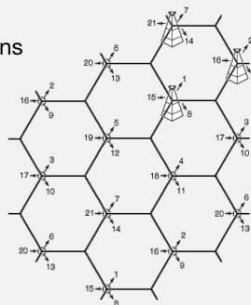
Cellular Network Standards

GSM

☑ Global System for Mobile Communications

　☑ Mobile networking standard

☑ 90% of the market

　☑ Originally an EU standard - Worldwide coverage

☑ Used by AT&T and T-Mobile in the United States

　☑ Move your SIM card (Subscriber Identity Module) from phone to phone

☑ Original GSM standard uses TDMA to multiplex calls

　☑ Everyone gets a little slice of time

Slide 33

Cellular Network Standards

Time-Division Multiple Access (TDMA)

☑ Multiple streams are combined into a single stream, and then broken out again - "Muxing"

Time-division multiplexing (TDM)

Multiplexer

Demultiplexer

Slide 34
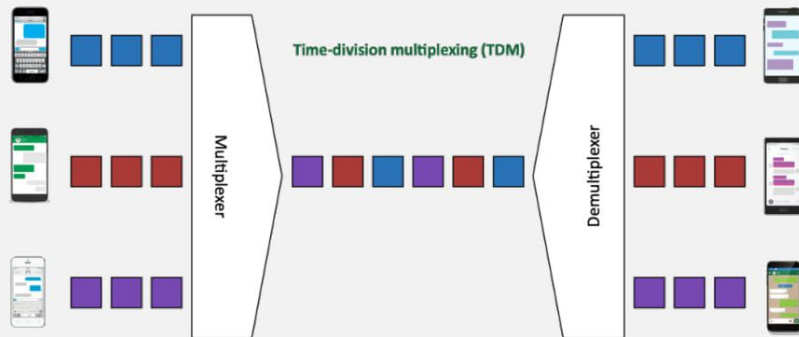
Cellular Network Standards

CDMA

☑ Code Division Multiple Access

 ☑ Everyone communicates at the same time

 ☑ Each call uses a different code

 ☑ The codes are used to filter each call on the receiving side

☑ Used by Verizon and Sprint

 ☑ Handsets are controlled by the network provider

 ☑ Not much adoption elsewhere

Slide 35

Cellular Network Standards

4G and LTE

☑ Long Term Evolution (LTE) - A "4G" technology

 ☑ Converged standard (GSM and CDMA providers)

 ☑ Based on GSM and EDGE (Enhanced Data Rates for GSM Evolution

 ☑ Standard supports download rates of 150 Mbit/s

☑ LTE Advanced (LTE-A)

 ☑ Standard supports download rates of 300 Mbit/s

Slide 36

Wireless Network Technologies

2.4 GHz Spectrum for 802.11 - North America

IEEE Channel #   1   6   11
20 MHz
2412 MHz   2482 MHz

5 GHz Spectrum for 802.11 - North America

IEEE Channel #   36 40 44 48 52 56 60 64 68 72 76 80 84 88 92 96 100 104 108 112 116 120 124 128 132 136 140 144 149 153 157 161 165 169 173 177
20 MHz
40 MHz
80 MHz
160 MHz

5350 MHz   UNII-1   5250 MHz   UNII-2   5350 MHz   5470 MHz   UNII-2   5725 MHz   UNII-3   5825 MHz   5925 MHz

■ Available channels
■ New channels added in April 2014
■ Previously indoor channels, usable outdoors after April 2014
■ Frequencies not available for 802.11

Wireless Network Technologies

802.11 technologies
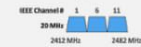
☑ Frequency

    ☑ 2.4 GHz or 5 GHz

    ☑ And sometimes both

☑ Channels

    ☑ Groups of frequencies, numbered by the IEEE

    ☑ Non-overlapping channels would be necessary

☑ Bandwidth

    ☑ Amount of frequency in use

    ☑ 20 MHz, 40 MHz, 80 MHz, 160 MHz

Wireless Network Technologies

☑ Power level controls   ☑ Directional antennas

☑ Omnidirectional antennas   ☑ Wireless survey tools

CSF 432: Intro to Network and System Security

Week 05 - Review

Michael Conti

Department of Computer Science and Statistics
University of Rhode Island

Fall 2020