CSF 432: Intro to Network and System Security

Week 01 - Review

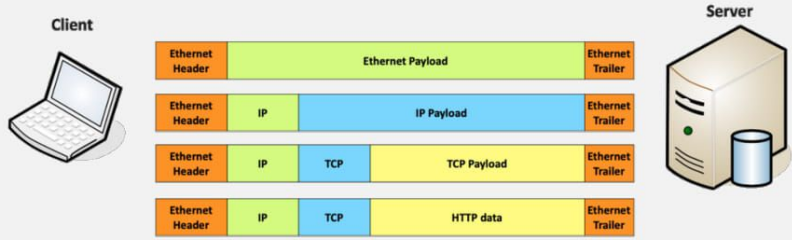
Michael Conti

Department of Computer Science and Statistics
University of Rhode Island

Fall 2020

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

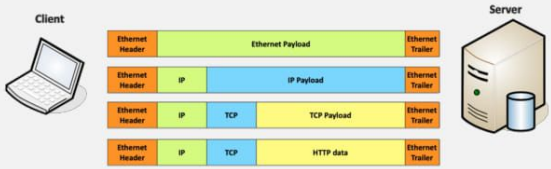
Introduction to IP



Introduction to IP

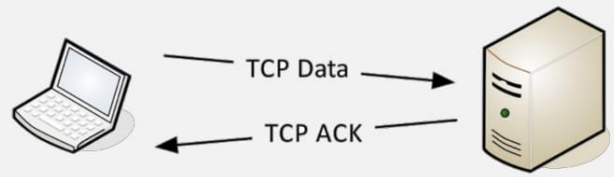
A Series of Moving Vans

- Efficiently move large amounts of data
  - Use a shipping truck
- The network topology is the road
  - Ethernet, DSL, coax cable
- The truck is the Internet Protocol (IP)
  - We've designed the roads for this truck
- The boxes hold your data
  - Boxes of TCP and UDP
- Inside the boxes are more things
  - Application information

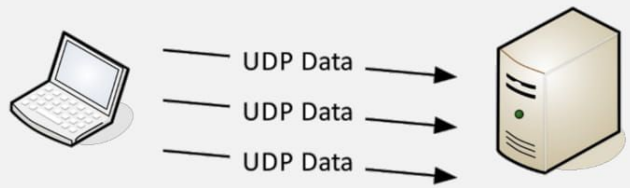


TCP and UDP

TCP - Transmission Control Protocol Communication



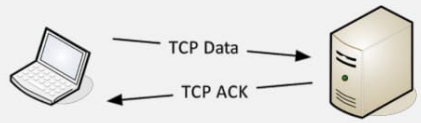
UDP - User Datagram Protocol Communication



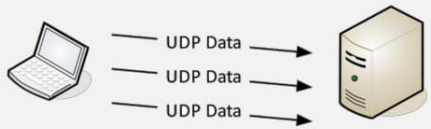
TCP and UDP

- Transported inside of IP
  - Encapsulated by the IP protocol
- Two ways to move data from place to place
  - Different features for different applications
- OSI Layer 4
  - The transport layer
- Multiplexing
  - Use many different applications at the same time (TCP and UDP)

TCP - Transmission Control Protocol Communication



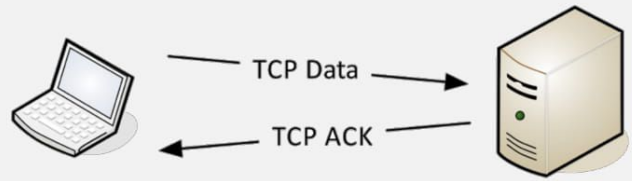
UDP - User Datagram Protocol Communication



TCP - Transmission Control Protocol Communication

- Connection-oriented
  - A formal connection setup and close
- Flow Control
  - The receiver can manage how much data is sent
- "Reliable" delivery
  - Different features for different applications
  - Recovery from errors
  - Can manage out-of-order messages or retransmissions

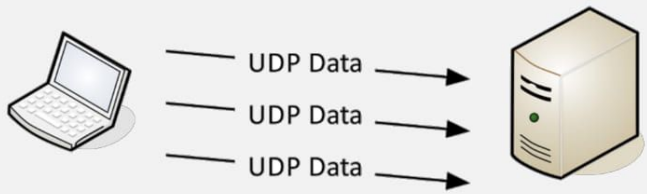
TCP - Transmission Control Protocol Communication



UDP - User Datagram Protocol Communication

- Connectionless
  - No formal open or close to the connection
- "Unreliable" delivery - No error recovery
  - No reordering of data or retransmissions
- No flow control
  - Sender determines the amount of data transmitted

UDP - User Datagram Protocol Communication



Common Ports

Common Network Protocols			
SSH	tcp/22	Secure Shell	Encrypted console login
DNS	udp/53	Domain Name System	Convert domain names to IP addresses
SMTP	tcp/25	Simple Mail Transfer Protocol	Transfer email between mail servers
SFTP	tcp/22	Secure FTP	Secure file transfer
FTP	tcp/20, tcp/21	File Transfer Protocol	Sends and receives files between systems
TFTP	udp/69	Trivial File Transfer Protocol	A very simple file transfer application
Telnet	tcp/23	Telecommunication Network	Remote console login to network devices
DHCP	udp/67, udp/68	Dynamic Host Configuration Protocol	Automated IP addressing and configuration
HTTP	tcp/80	Hypertext Transfer Protocol	Web server communication
HTTPS	tcp/443	Hypertext Transfer Protocol Secure	Web server communication with encryption
SNMP	udp/161	Simple Network Management Protocol	Gather statistics and manage network devices
RDP	tcp/3389	Remote Desktop Protocol	Graphical display of remote device
NTP	udp/123	Network Time Protocol	Synchronize clocks
SIP	tcp/5060-5061	Session Initiation Protocol	Voice over IP signaling protocol
SMB	tcp/445	Server Message Block	Windows file transfers and printer sharing
POP3	tcp/110	Post Office Protocol version 3	Receive mail into a mail client
IMAP4	tcp/143	Internet Message Access Protocol v4	A newer mail client protocol
LDAP	tcp/389	Lightweight Directory Access Protocol	Communicate with network directories
LDAPS	tcp/636	Lightweight Directory Access Protocol Secure	LDAP over SSL
H.323	tcp/1720	ITU Telecommunication H.32x protocol series	Voice over IP signaling

Common Ports

SSH - Secure Shell

- Encrypted communication link - tcp/22
- Looks and acts the same as Telnet

DNS - Domain Name System

- Converts names to IP addresses - udp/53
  - www.uri.edu = 64.131.77.69
- These are very critical resources
    - Usually multiple DNS servers are in production

SMTP - Simple Mail Transfer Protocol

- Server to server email transfer - tcp/25
  - Also used to send mail from a device to a mail server
- Commonly configured on mobile devices and email clients
- Other protocols are used for clients to receive email
  - eg. IMAP, POP3

Common Ports

SFTP - Secure FTP

- Uses the SSH File Transfer Protocol - tcp/22
- Provides file system functionality
- Resuming interrupted transfers, directory listings,
- remote file removal

Telnet

- Telnet – Telecommunication Network - tcp/23 Login to devices remotely
- Console access
- In-the-clear communication
- Not the best choice for production systems

FTP – File Transfer Protocol

- tcp/20 (active mode data), tcp/21 (control)
- Transfers files between systems
- Authenticates with a username and password
- Full-featured functionality (list, add, delete, etc.)

TFTP – Trivial File Transfer Protocol

- udp/69
- Very simple file transfer application
  - Read files and write files
- No authentication - Not used on production systems

Common Ports

DHCP - Dynamic Host Configuration Protocol

- Automated configuration of IP address, subnet mask and other options
  - udp/67, udp/68 - Requires a DHCP server
- Dynamic / Pooled
  - IP addresses are assigned in real-time from a pool
  - Each system is given a lease
  - Must renew at set intervals
- Reserved
  - Addresses are assigned by MAC address
  - Quickly manage addresses from one location

HTTP and HTTPS

- Hypertext Transfer Protocol
  - Communication in the browser
  - And by other applications
- In the clear or encrypted
  - Supported by nearly all web servers and clients

Common Ports

SNMP - Simple Network Management Protocol

- Gather statistics from network devices udp/161
- v1 – The original
  - Structured tables, in-the-clear
- v2 – A good step ahead
  - Data type enhancements, bulk transfers Still in-the-clear
- v3 – The new standard
  - Message integrity, authentication, encryption

RDP - Remote Desktop Protocol

- Share a desktop from a remote location over tcp/3389 Remote Desktop
- Services on many Windows versions
- Can connect to an entire desktop or just an application
- Clients for Windows, MacOS, Linux, iPhone, and others

Common Ports

NTP - Network Time Protocol

- Switches, routers, firewalls, servers, workstations
  - Every device has its own clock - udp/123
- Synchronizing the clocks becomes critical
  - Log files, authentication information, outage details
- Automatic updates
  - No flashing 12:00 lights
- Flexible - You control how clocks are updated
- Very accurate
  - Accuracy is better than 1 millisecond

SIP - Session Initiation Protocol

- Voice over IP (VoIP) signaling
  - tcp/5060 and tcp/5061
- Setup and manage VoIP sessions
  - Call, ring, hang up
- Extend voice communication
  - Video conferencing, instant messaging, file transfer, etc.

Common Ports

SMB - Server Message Block

- Protocol used by Microsoft Windows
  - File sharing, printer sharing
  - Also called CIFS (Common Internet File System)
- Direct over tcp/445 (NetBIOS-less)
  - Direct SMB communication over TCP without the NetBIOS transport

POP/IMAP

- Receive emails from an email server
  - Authenticate and transfer
- POP3 - Post office Protocol version 3 - tcp/110
  - Basic mail transfer functionality
- IMAP4 - Internet Message Access Protocol v4 - tcp/143
  - Manage email inbox from multiple clients

Common Ports

LDAP/LDAPS

- LDAP (Lightweight Directory Access Protocol) - tcp/389
  - Store and retrieve information in a network directory
- LDAPS (LDAP Secure) - tcp/636
  - A non-standard implementation of LDAP over SSL

H.323

- Voice over IP (VoIP) signaling - tcp/1720
  - ITU Telecommunication H.32x protocol series
- Setup and manage VoIP sessions
  - Call, ring, hang up
- One of the earliest VoIP standards
  - Still in use today

Understanding the OSI Model

Layer 7 - Application	The layer we see - Google Mail, Twitter, Facebook
Layer 6 - Presentation	Encoding and encryption (SSL/TLS)
Layer 5 - Session	Communication between devices (Control protocols, tunneling protocols)
Layer 4 - Transport	The “post office” layer (TCP segment, UDP datagram)
Layer 3 - Network	The routing layer (IP address, router, packet)
Layer 2 - Data Link	The switching layer (Frame, MAC address, EUI-48, EUI-64, Switch)
Layer 1 - Physical	Signaling, cabling, connectors (Cable, NIC, Hub)

OSI Model

Open Systems Interconnection Reference Model

- It's a guide (thus the term "model")
- Don't get wrapped up in the details
- This is not the OSI protocol suite
- Most of the OSI protocols didn't catch on
- There are unique protocols at every layer
- You'll refer to this model for the rest of your career

Layer 7 - Application	The layer we see - Google Mail, Twitter, Facebook
Layer 6 - Presentation	Encoding and encryption (SSL/TLS)
Layer 5 - Session	Communication between devices (Control protocols, tunneling protocols)
Layer 4 - Transport	The "post office" layer (TCP segment, UDP datagram)
Layer 3 - Network	The routing layer (IP address, router, packet)
Layer 2 - Data Link	The switching layer (Frame, MAC address, EUI-48, EUI-64, Switch)
Layer 1 - Physical	Signaling, cabling, connectors (Cable, NIC, Hub)

OSI Model

Layer 1 - The Physical Layer

- The physics of the network
  - Signaling, cabling, connectors
  - This layer isn't about protocols
- You have a physical layer problem."
  - Fix your cabling, punch-downs, etc.
  - Run loopback tests, test/ replace cables, swap adapter cards

Layer 2 - Data Link Layer

- The basic network "language"
  - The foundation of communication at the data link layer
- Data Link Control (DLC) protocols
  - MAC (Media Access Control) address on Ethernet
- The "switching" layer

OSI Model

Layer 3 - The Network Layer

- The "routing" layer
- Internet Protocol (IP)
- Fragments frames to traverse different networks

Layer 4 - Transport Layer

- The "post office" layer
  - Parcels and letters
- TCP and UDP

Layer 5 - Session Layer

- Communication management between devices Start, stop, restart
- Half-duplex, full-duplex
- Control protocols, tunneling protocols

Hint: What is IP Fragmentation?

Fragments are always in multiples of 8 because of the number of fragmentation offset bits in the IP header

OSI Model

Layer 6 - Presentation Layer

- Character encoding
- Application encryption
- Often combined with the Application Layer

Layer 7 - Application Layer

- The layer we see: HTTP, FTP, DNS, POP3

OSI Mnemonics

- **P**lease **D**o **N**ot **T**rust **S**ales **P**erson's **A**nswers
- **A**ll **P**eople **S**eem **T**o **N**eed **D**ata **P**rocessing
- **P**lease **D**o **N**ot **T**hrow **S**ausage **P**izza **A**way!

Physical - **D**ataLink - **N**etwork - **T**ransport - **S**ession - **P**resentation - **A**pplication

Introduction to Ethernet

Field	Bytes	Description
Preamble	7	56 alternating ones and zeros used for synchronization (101010...)
SFD	1	Start Frame Delimiter - designates the end of the preamble (10101011)
Destination MAC Address	6	Ethernet MAC address of the destination device
Source MAC Address	6	Ethernet MAC address of the source device
EtherType	2	Describes the data contained the payload
Payload	46 - 1500	Layer 3 and higher data
FCS	4	Frame Check Sequence - CRC checksum of the frame

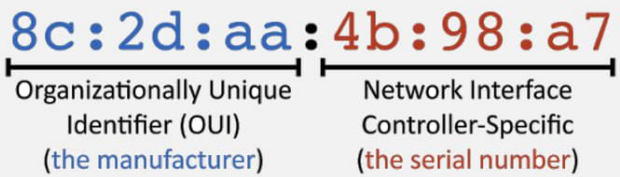
Field	Bytes	Description
Preamble	7	56 alternating ones and zeros used for synchronization (101010...)
SFD	1	Start Frame Delimiter - designates the end of the preamble (10101011)
Destination MAC Address	6	Ethernet MAC address of the destination device
Source MAC Address	6	Ethernet MAC address of the source device
EtherType	2	Describes the data contained the payload
Payload	46 - 1500	Layer 3 and higher data
FCS	4	Frame Check Sequence - CRC checksum of the frame

The MAC address

- Ethernet Media Access Control address
  - The "physical" address of a network adapter
  - Unique to a device
- 48 bits / 6 bytes long
  - Displayed in hexadecimal

Half-duplex

- A device cannot send and receive simultaneously
- All LAN hubs are half-duplex devices
- Switch interfaces can be configured as half-duplex, but usually only when connecting to another half-duplex device

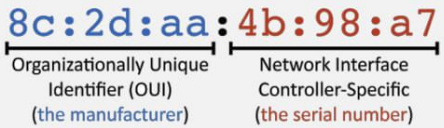


Full-duplex

- Data can be sent and received at the same time
- A properly configured switch interface will be set to full-duplex

CSMA/CD

- CS - Carrier Sense
  - Is there a carrier? Is anyone communicating?
- MA - Multiple Access
  - More than one device on the network
- CD - Collision Detect
  - Collision - Two stations talking at once
  - Identify when data gets garbled
- Half-duplex Ethernet - not used any longer



Introduction to Ethernet

CSMA/CD operation

- Listen for an opening
  - Don't transmit if the network is already busy
- Send a frame of data
  - You send data whenever you can
  - There's no queue or prioritization
- If a collision occurs
  - Transmit a jam signal to let everyone know a collision has occurred
  - Wait a random amount of time, then retry

CSMA/CA

- CA - Collision Avoidance
- Collision detection isn't possible
- Common to see RTS/CTS
- Solves the "hidden node" problem

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

Organizationally Unique Identifier (OUI) (the manufacturer)

Network Interface Controller-Specific (the serial number)

Network Switching

Network Switching

The Switch

- Forward or drop frames
  - Based on the destination MAC address
- Gather a constantly updating list of MAC addresses
  - Builds the list based on the source MAC address of incoming traffic
- Maintain a loop-free environment
  - Using Spanning Tree Protocol (STP)

Learning the MACs

- Switches examine incoming traffic
  - Makes a note of the source MAC address
- Adds unknown MAC addresses to the MAC address table
  - Sets the output interface to the received interface

Flooding for unknown Macs

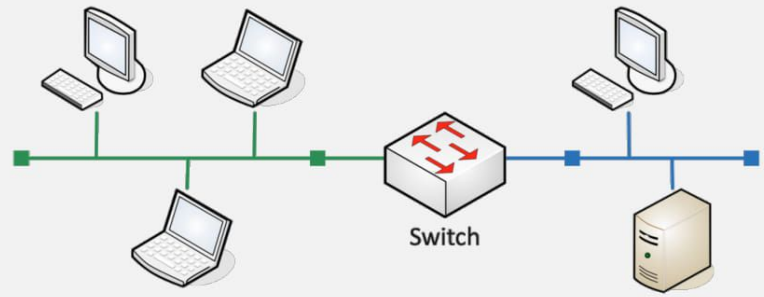
- The switch doesn't always have a MAC address in the table
- When in doubt, send the frame to everyone

Address Resolution Protocol

- Determine a MAC address based on an IP address
  - You need the hardware address to communicate

View local ARP table with command: **arp -a**

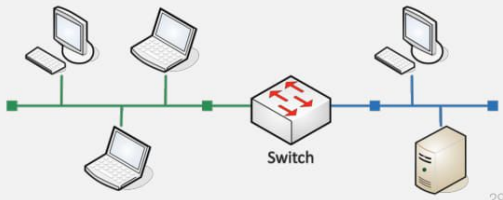
Collision Domains



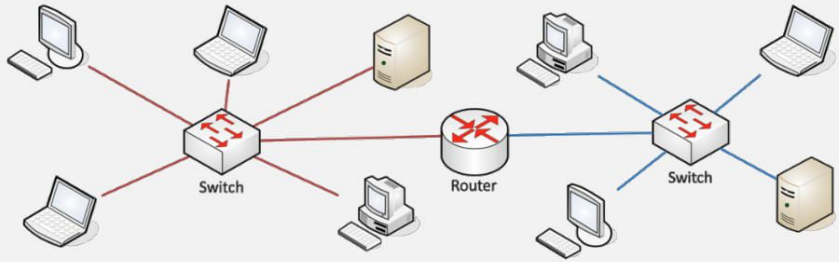
Collision domains

Collision domains

- Separated by switch/bridge interfaces
- A historical footnote
  - It's difficult to find a collision these days
- The network was one big segment
  - Everyone heard everyone else's signals
  - One big conference call
- Only one station can "talk" at a time
  - Is the line clear? Ok, I can talk.
  - Carrier Sense Multiple Access (CSMA)
- When two people spoke at the same time, there was a collision
  - Collision Detection (CD) - Send the jam signal



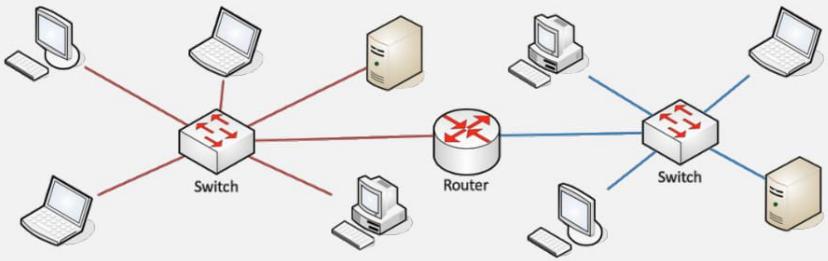
Broadcast Domains



Broadcast Domains

Broadcast Domains

- Separated by router interfaces
- Spread the word!
  - Everyone must know!
  - ARP probes, operating system notifications
- How far can a broadcast go?
  - Passed by a switch/bridge
  - Stops at the router
- This can be important
  - More devices, more broadcasts



CSF 432: Intro to Network and System Security

Week 01 - 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