CSF 432: Intro to Network and System Security

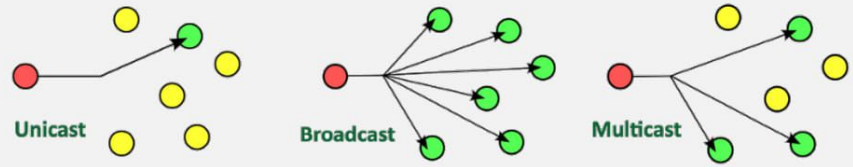
Week 02 - Review

Michael Conti

Department of Computer Science and Statistics
University of Rhode Island

Fall 2020

Unicasts, Broadcasts, and Multicasts



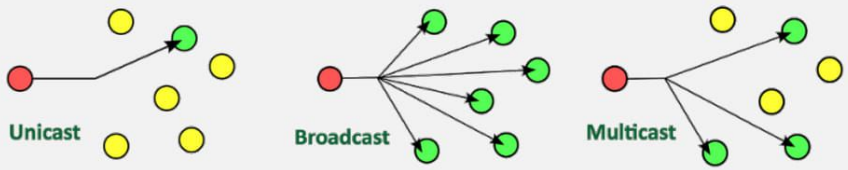
Unicasts, Broadcasts, and Multicasts

Unicast

- One station sending information to another station
- Send information between two systems
- Web surfing, file transfers
- Does not scale optimally for streaming media

Multicast

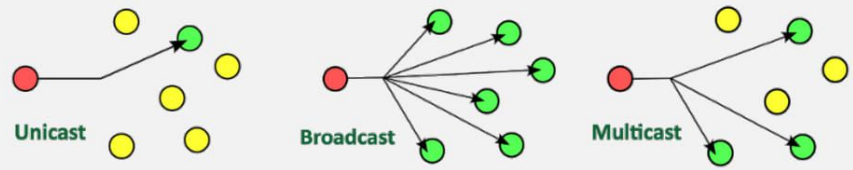
- Delivery of information to interested systems
  - One to many
- Multimedia delivery, stock exchanges
- Very specialized
  - Difficult to scale across large networks



Unicasts, Broadcasts, and Multicasts

Broadcasts

- Send information to everyone at once
- One packet, received by everyone
- Limited scope - the broadcast domain
- Routing updates, ARP requests
- Not used in IPv6 - focus on multicast



Protocol Data Units

Protocol Data Units

PDU (Protocol Data Unit)

- A unit of transmission
  - A different group of data at different OSI layers
- Ethernet operates on a frame of data
  - It has no idea what's inside
- IP operates on a packet of data
  - Inside is TCP or UDP, but IP doesn't know that
- TCP or UDP PDU - TCP segment, UDP datagram

Protocol Data Units

Maximum Transmission Unit (MTU)

- Maximum IP packet to transmit - but not fragment
- Fragmentation slows things down
  - Losing a fragment loses an entire packet
  - Requires overhead along the path
- Difficult to know the MTU all the way through the path
  - Automated methods are often inaccurate, especially when ICMP is filtered

Protocol Data Units

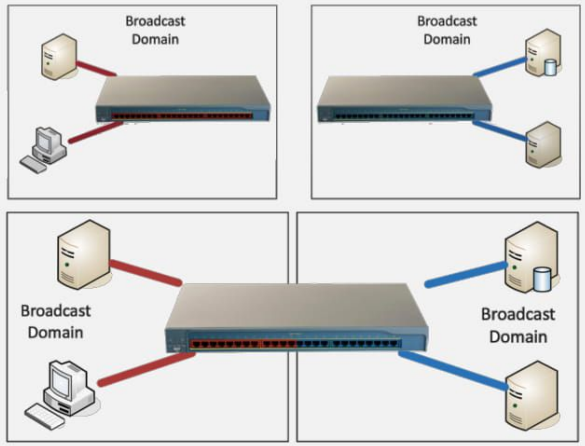
Troubleshooting MTU

- MTU sizes are usually configured once
  - Based on the network infrastructure and don't change often
- A significant concern for tunneled traffic
  - The tunnel may be smaller than your local Ethernet segment
- What if you send packets with Don't Fragment (DF) set?
  - Routers will respond back and tell you to fragment
  - Hope you get the ICMP message!
- Troubleshoot using ping
  - Ping with DF and force a maximum size of 1472 bytes
  - 1500 bytes - 8 byte ICMP header - 20 bytes IP address = 1472 bytes

Windows terminal command:

```
ping -f -l 1472 8.8.8.8
```

Network Segmentation



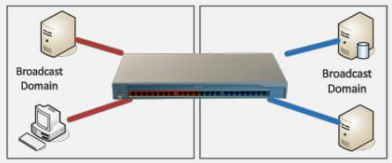
Network Segmentation

LANs

- Local Area Networks
  - A group of devices in the same broadcast domain

Virtual LANs

- Virtual Local Area Networks
  - A group of devices in the same broadcast domain
  - Separated logically instead of physically



Network Segmentation

802.1Q trunking

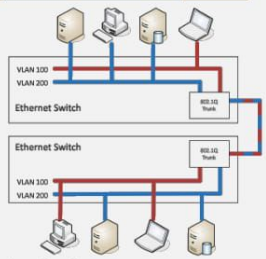
- Take a normal Ethernet frame

Preamble	SFD	Destination MAC	Source MAC	Type	Payload	FCS

- Add a VLAN header in the frame

Preamble	SFD	Destination MAC	Source MAC	VLAN	Type	Payload	FCS

- VLAN IDs - 12 bits long, 4,094 VLANs
  - "Normal range" - 1 through 1005
  - "Extended range" - 1006 through 4094
  - 0 and 4,095 are reserved VLAN numbers
- Before 802.1Q, there was ISL (Inter-Switch Link)
  - ISL is no longer used; everyone now uses the 802.1Q standard



Spanning Tree Protocol

Spanning Tree Protocol

Loop protection

- Connect two switches to each other
  - They'll send traffic back and forth forever
  - There's no "counting" mechanism at the MAC layer
- This is an easy way to bring down a network
  - And somewhat difficult to troubleshoot
  - Relatively easy to resolve
- IEEE standard 802.1D to prevent loops in bridged (switched) networks (1990)

Switching Operation

- Forwarding decisions made by MAC address
  - Keeps a big table of MAC address that have been seen
  - All forwarding decisions are filtered through this list
- If the destination MAC is unknown, the frame is flooded
  - Sent to every switch port in the local subnet/VLAN
  - Hopefully the destination station will respond
- Flooding is hopefully a temporary process
  - Directed traffic resumes when the MAC is seen

Protocol Data Units

STP port states

- Blocking - Not forwarding to prevent a loop
- Listening - Not forwarding and cleaning the MAC table
- Learning - Not forwarding and adding to the MAC table
- Forwarding - Data passes through and is fully operational
- Disabled - Administrator has turned off the port

RSTP (802.1w)

- Rapid Spanning Tree Protocol (802.1w)
  - A much-needed updated of STP
  - This is the latest standard
- Faster convergence
  - From 30 to 50 seconds to 6 seconds
- Backwards-compatible with 802.1D STP
  - You can mix both in your network
- Very similar process
  - An update, not a wholesale change

Switch Interface Properties

Switch Interface Properties

Basic Interface Configuration

- Speed and duplex
  - Speed: 10 / 100 /1,000
  - Duplex: Half/Full
  - Automatic and manual
  - Needs to match on both sides
- IP address management
  - Layer 3 interfaces
  - VLAN interfaces
  - Management interfaces
  - IP address, subnet mask/CIDR block, default gateway, DNS (optional)

VLANs

- VLAN assignment
  - Each device port should be assigned a VLAN
- Trunking
  - Connecting switches together - Multiple VLANs in a single link
- Tagged and untagged VLANs
  - A non-tagged frame is on the default VLAN (Also called the native VLAN)
- Trunk ports will tag the outgoing frames
  - And remove the tag on incoming frames

Switch Interface Properties

Powering devices

- Power provided on an Ethernet cable
  - One wire for both network and electricity
  - Phones, cameras, wireless access points
- Power provided at the switch
  - Built-in power - Endspans
  - In-line power injector - Midspans
- Power modes
  - Mode A - Power on the data pairs
  - Mode B - Power on the spare pairs

PoE and POE+

- PoE: IEEE 802.3af-2003
  - The original PoE specification
  - Included in 802.3at
  - Now part of 802.3-2012
  - 15.4 watts DC power
  - Maximum current of 350 mA
- POE+: IEEE 802.3at-2009
  - The updated PoE specification
  - Now also part of 802.3-2012
  - 25.5 watts DC power
  - Maximum current of 600 mA

Switch Interface Properties

DMZ

- Demilitarized zone
  - An additional layer of security between the Internet and you

Port mirroring

- Examine a copy of the traffic
  - Port mirror (SPAN), network tap
- No way to block (prevent) traffic

Static and Dynamic Routing

Static and Dynamic Routing

Routing

- Send IP packets across the network
  - Forwarding decisions are based on destination IP address
- Each router only knows the next step
  - The packet asks for directions every hop along the way
  - The list of directions is held in a routing table
- Different topologies use different data link protocols
  - Ethernet, HDLC, etc.
- Each router rewrites the frame to add its own data-link header
  - The IP packet remains intact

Static and Dynamic Routing

Static routing

- Administratively define the routes - You're in control
- Advantages
  - Easy to configure and manage on smaller networks
  - No overhead from routing protocols (CPU, memory, bandwidth)
  - Easy to configure on sub networks (only one way out)
  - More secure - no routing protocols to analyze
- Disadvantages
  - Difficult to administer on larger networks
  - No automatic method to prevent routing loops
  - If there's a network change, you have to manually update the routes
  - No automatic rerouting if an outage occurs

Static and Dynamic Routing

Dynamic routing

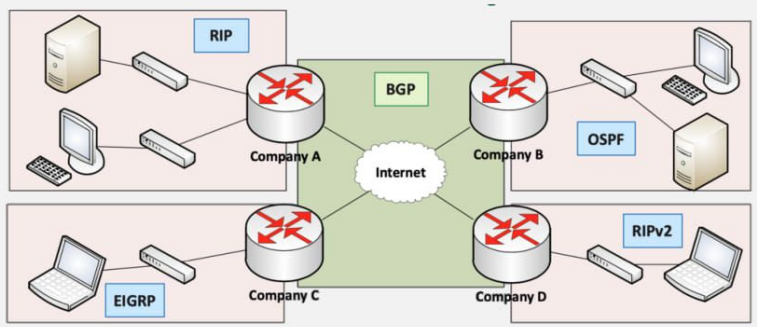
- Routers send routes to other routers
  - Routing tables are updated in (almost) real-time
- Advantages
  - No manual route calculations or management
  - New routes are populated automatically
  - Very scalable
- Disadvantages
  - Some router overhead required
  - Requires some initial configuration to work properly protocols to analyze

Static and Dynamic Routing

Default route

- A route when no other route matches
  - The "gateway of last resort"
- A remote site may have only one route
  - Go that way -> rest of the world
- Can dramatically simplify the routing process
  - Works in conjunction with all other routing methods

IGP and EGP



IGP and EGP

AS (Autonomous System)

- Autonomous
  - Existing as an independent entity
- Group of IP routes under common control
- RFC 1930, Section 3: Definitions
  - "An AS is a connected group of one or more IP prefixes run by one or more network operators which has a SINGLE and CLEARLY DEFINED routing policy."
- Important point of reference for discussing Interior Gateway Protocols and Exterior Gateway Protocols

IGP and EGP

IGP (Interior Gateway Protocol)

- Used within a single autonomous system (AS)
  - Not intended to route between AS
  - That's why there's Exterior Gateway Protocols (EGPs)
- IPv4 dynamic routing
  - OSPFv2 (Open Shortest Path First)
  - RIPv2 (Routing Information Protocol version 2)
  - EIGRP (Enhanced Interior Gateway Routing Protocol)
- IPv6 dynamic routing
  - OSPFv3
  - EIGRP for IPv6
  - RIPng (RIP next generation)

IGP and EGP

EGP (Exterior Gateway Protocol)

- Used to route between autonomous systems
- Leverages the IGP at the AS to handle local routing
- BGP (Border Gateway Protocol)
- Many organizations use BGP as their EGP

Dynamic Routing Protocols

Dynamic Routing Protocols

Dynamic routing protocols

- Listen for subnet information from other routers
  - Sent from router to router
- Provide subnet information to other routers
  - Tell other routers what you know
- Determine the best path based on the gathered information
  - Every routing protocol has its own way of doing this
- When network changes occur, update the available routes
  - Different convergence process for every dynamic routing protocol

Dynamic Routing Protocols

Which routing protocol to use?

- What exactly is a route?
  - Is it based on the state of the link?
  - Is it based on how far away it is?
- How does the protocol determine the best path?
  - Some formula is applied to the criteria to create a metric
  - Rank the routes from best to worst
- Recover after a change to the network
  - Convergence time can vary widely between routing protocols
- Standard or proprietary protocol?
  - OSPF and RIP are standards, some functions of EIGRP are Cisco proprietary

Dynamic Routing Protocols

Distance-vector routing protocols

- Information passed between routers contains routing tables
  - How many “hops” away is another network?
  - The deciding “vector” is the “distance”
- Usually automatic
  - Very little configuration
- Good for smaller networks
  - Doesn’t scale well to very large networks
- RIP, RIPv2, EIGRP

Dynamic Routing Protocols

Link-state routing protocols

- Information passed between routers is related to the current connectivity
  - If it’s up, you can get there
  - If it’s down, you can’t
- Consider the speed of the link
  - Faster is always better, right?
- Very scalable
  - Used most often in large networks
- OSPF - Large, scalable routing protocol

Dynamic Routing Protocols

Hybrid routing protocols

- A little link-state, a little distance-vector
  - Not many examples of a hybrid routing protocol
- BGP (Border Gateway Protocol)
  - Determines route based on paths, network policies, or configured rule-sets

CSF 432: Intro to Network and System Security

Week 02 - 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