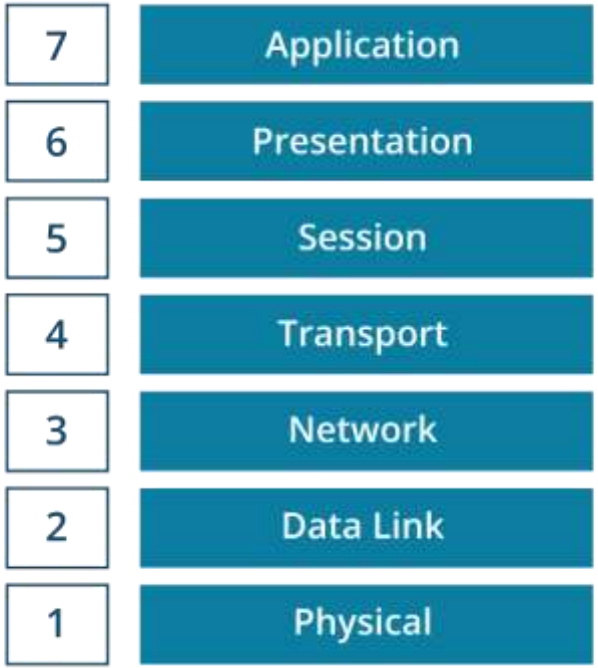
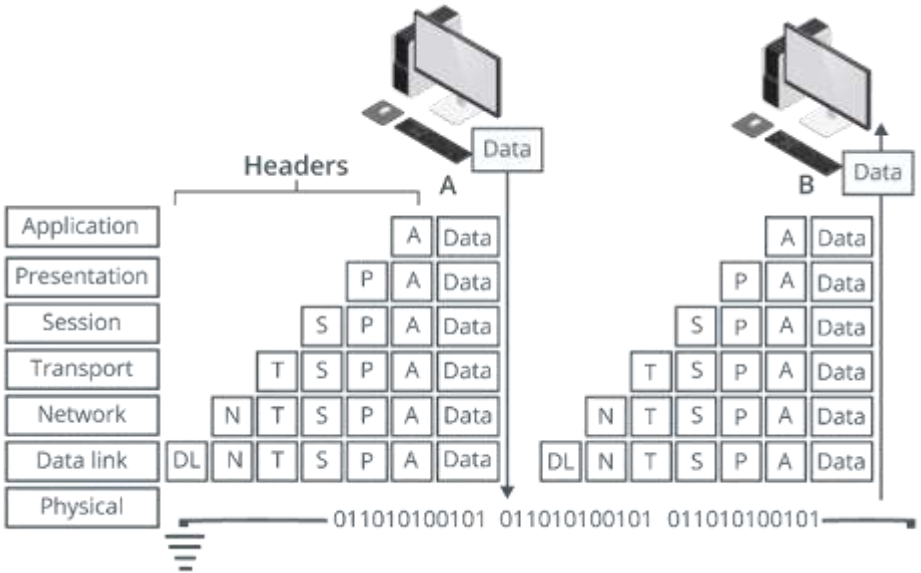
Open Systems Interconnection Model



Data Encapsulation and Decapsulation



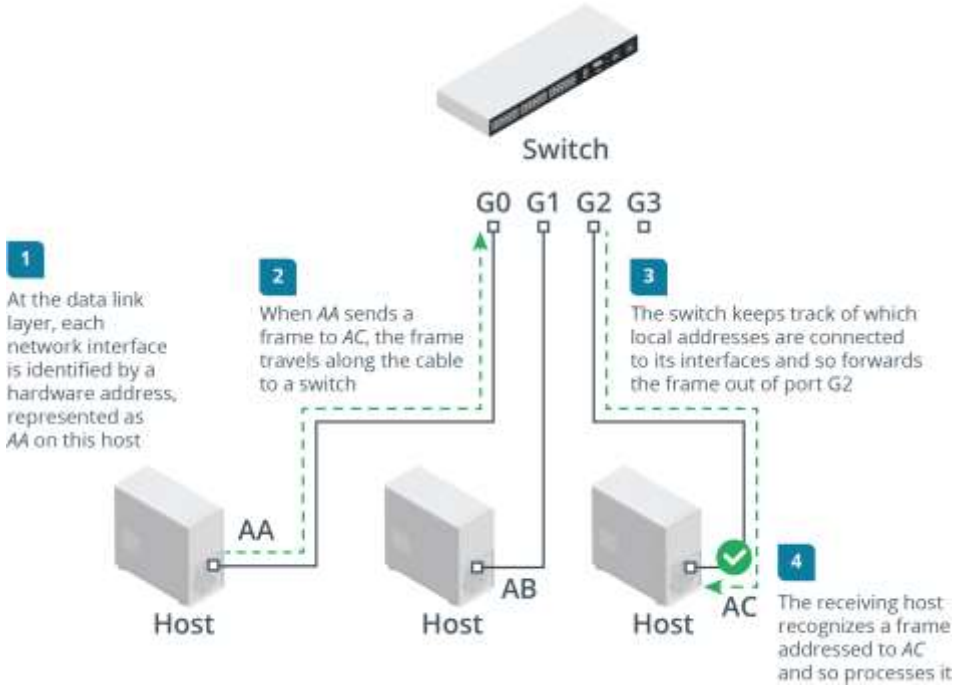
- Network protocol functions
  - Addressing
  - Encapsulation
- Protocol stack
  - Same layer interaction
  - Adjacent layer interaction
- Protocol Data Unit (PDU)
  - Headers
  - Payload/data

Layer 1—Physical

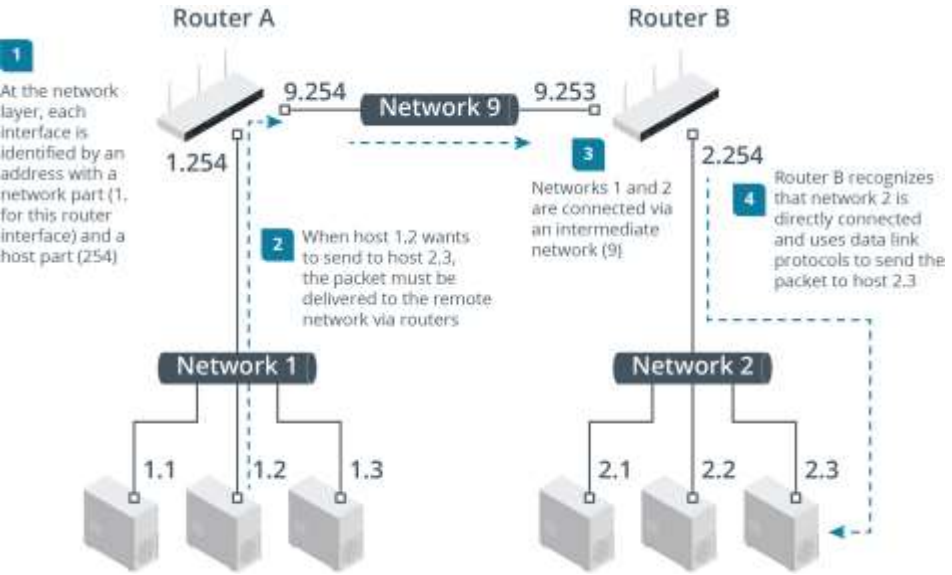
- Physical (PHY) layer transmission media types
  - Cabled
  - Wireless
- PHY layer features
  - Physical topology and segments
  - Physical interface and transmission of signals
  - Modulation and encoding
- Devices working at layer 1
  - Transceiver, repeater, hub, media converter, modem

Layer 2—Data Link

- Exchange PDUs as frames using hardware addresses within local segment
- Logical versus physical topology
- Intermediate systems versus end systems
- Devices working at layer 2
  - Network interface card (NIC), bridge, switch, wireless access point (AP)



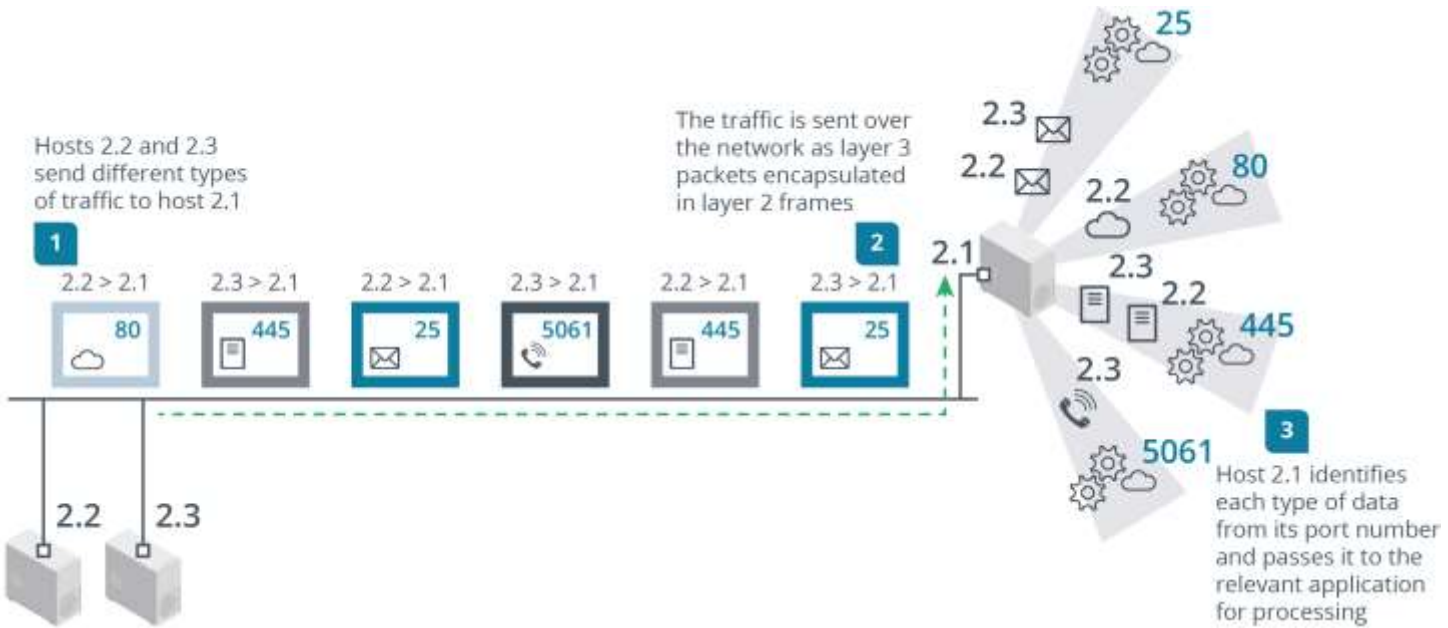
Layer 3—Network



- Network of networks or internetwork
- Forward datagrams/packets via routers using logical network addresses
- Can contain multiple segments using different physical layer specifications and layer 2 protocols
- Devices working at layer 3
  - Router, basic firewall

Layer 4—Transport

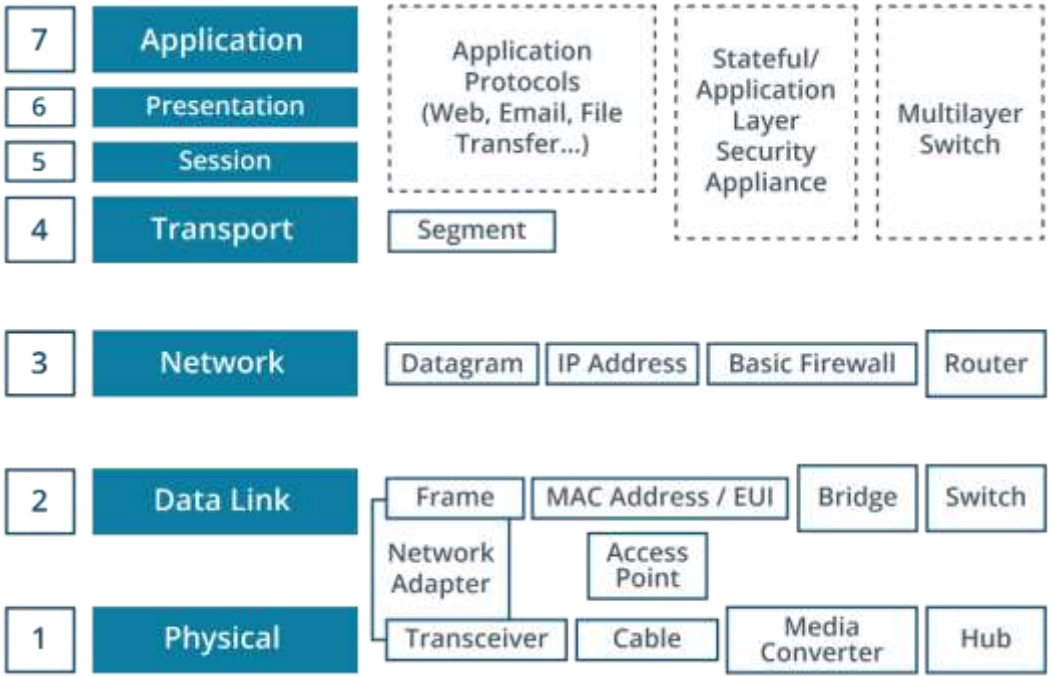
- Identify application data using port numbers
- Load balancer, advanced firewall, intrusion detection system (IDS)



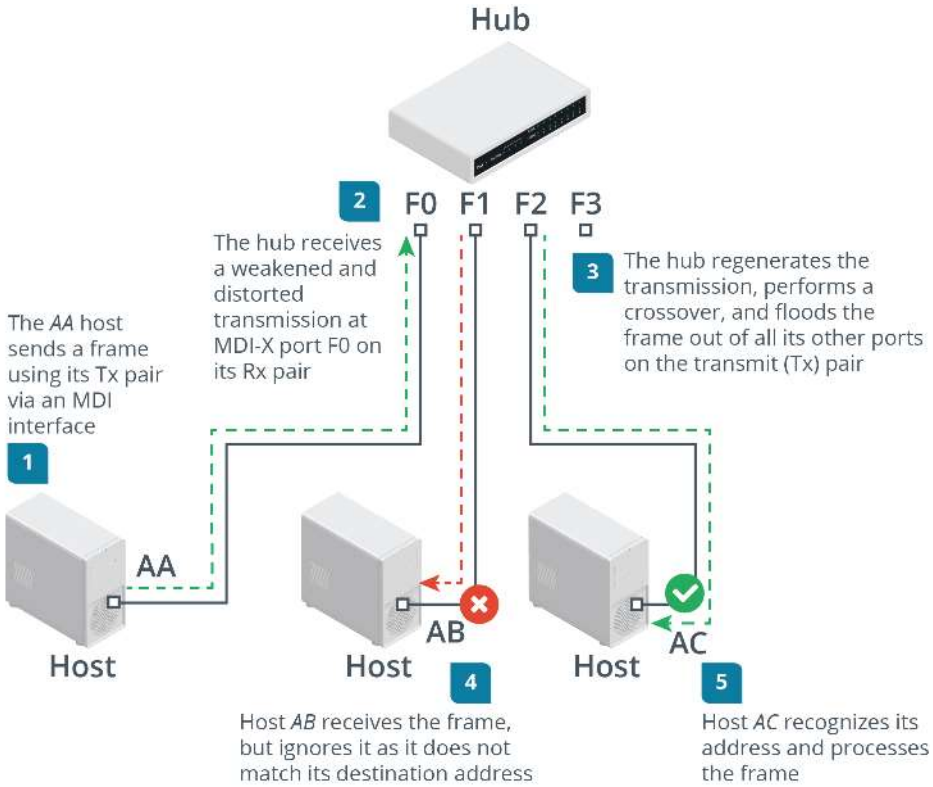
Upper Layers

- Layer 5—Session
  - Establish rules for exchange of messages and sequencing (dialog control)
- Layer 6—Presentation
  - Establish data formats (such as character sets)
- Layer 7—Application
  - Present requests and responses from server or client software with structured headers and data payload

OSI Model Summary



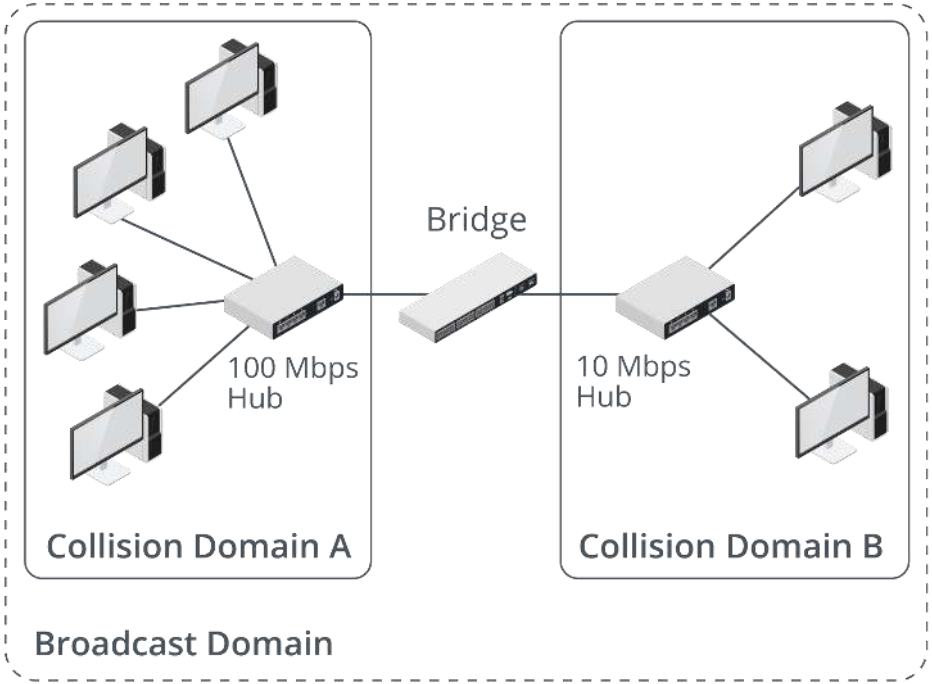
Hubs



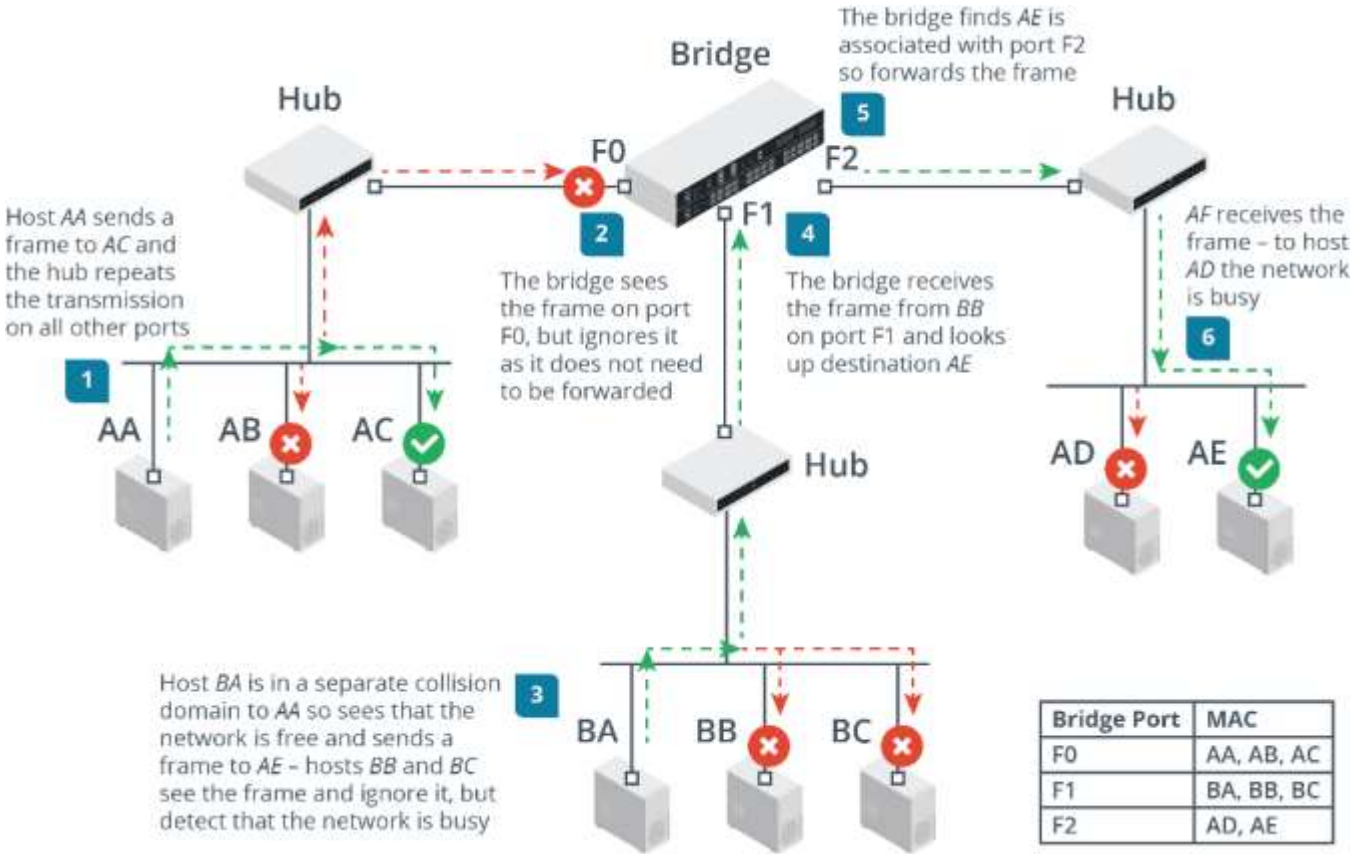
- Legacy intermediate system for Ethernet
- Multiport repeater working at physical layer
- All ports in the same collision domain
- Medium dependent interface (MDI)
  - End system to intermediate system
  - Transmit (Tx) --> Receive (Rx)
  - Hub ports are MDI-X (crossover)

Bridges (Slide 1 of 2)

- Works at data link layer (layer 2)
- Ports are in separate collision domains
- Ports are in same broadcast domain
- Bridge must track MAC addresses associated with each port



Bridges (Slide 2 of 2)

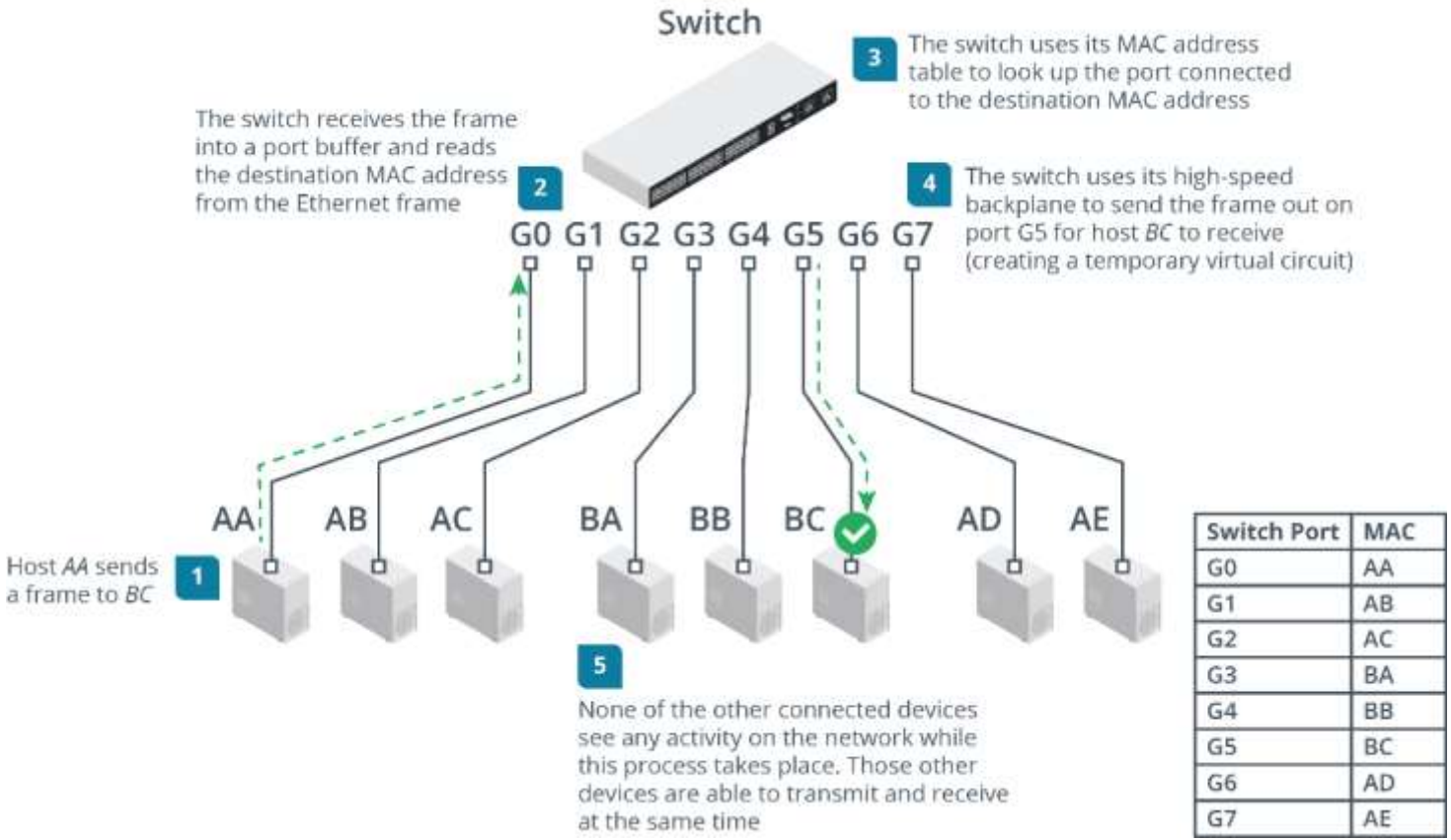


Bridge Port	MAC
F0	AA, AB, AC
F1	BA, BB, BC
F2	AD, AE

Layer 2 Switches (Slide 1 of 2)

- Replace hubs and bridges and eliminate performance drag from contention
- Each port is a separate collision domain
  - Microsegmentation
  - Allows full-duplex (depending on host NIC)
- All ports are in the same broadcast domain
  - Unless virtual LANs (VLANs) have been configured…

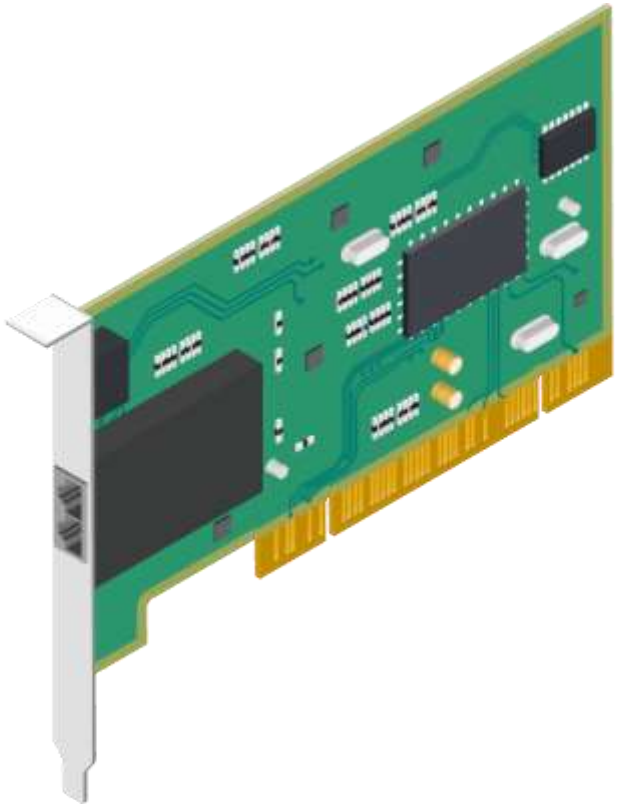
Layer 2 Switches (Slide 2 of 2)



Switch Port	MAC
G0	AA
G1	AB
G2	AC
G3	BA
G4	BB
G5	BC
G6	AD
G7	AE

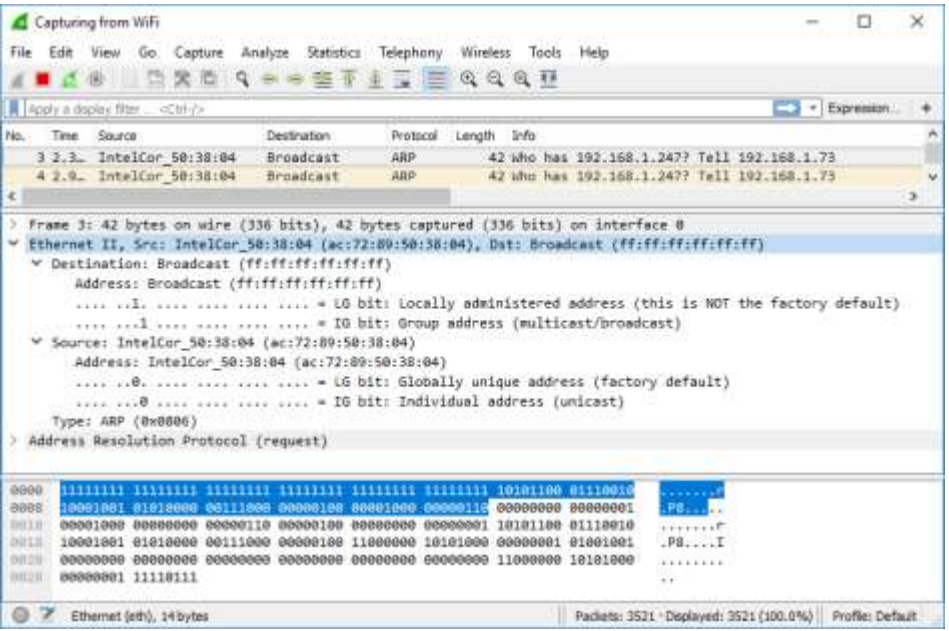
Network Interface Cards

- Network interface card/controller (NIC) or network adapter
- Transceiver component works at physical layer
  - Copper or fiber optic
  - Ethernet standard (10/100/1000 or 10G/40G)
  - Multi-port
- Card logic and driver work at data link layer
  - Ethernet framing
  - Local/hardware/physical address
    - Media access control (MAC) address/Ethernet Address (EA)/extended unique identifier (EUI)



Ethernet Frame Format

Media Access Control Address Format

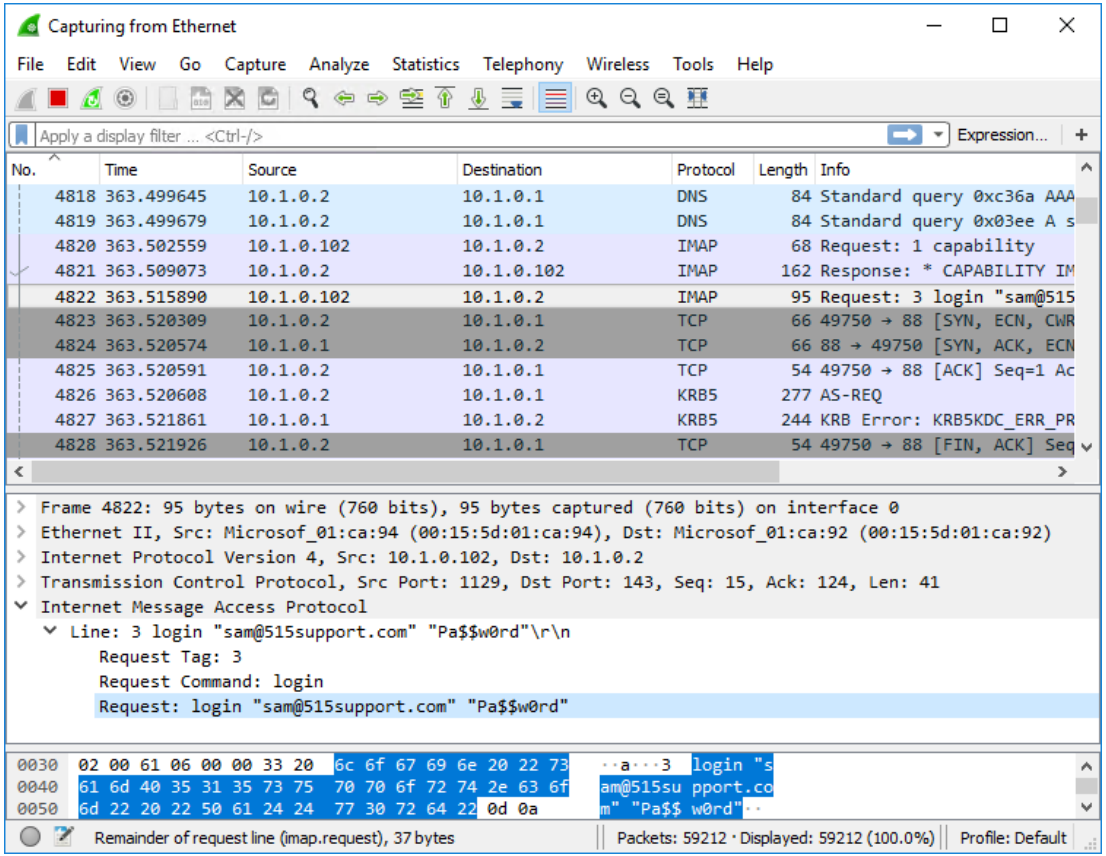


- 48 bit/6 byte ID expressed in hex notation
  - 00:60:8c:12:3a:bc
  - 00608c123abc
  - 0060.8c12.3abc
- Burned-in address
- Locally administered addresses
- Broadcast address
  - ff:ff:ff:ff:ff:ff

Packet Sniffers and Taps

- Protocol analyzer decodes (parses) frame and protocol headers and data
- Packet sniffer reads frames from the network
- Host-based capture
- Switched Port Analyzer (SPAN) / mirror port
- Test Access Point (TAP)
  - Passive versus active

Wireshark


Capturing from Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
4818 363.499645 10.1.0.2 10.1.0.1 DNS 84 Standard query 0xc36a AAA
4819 363.499679 10.1.0.2 10.1.0.1 DNS 84 Standard query 0x03ee A s
4820 363.502559 10.1.0.102 10.1.0.2 IMAP 68 Request: 1 capability
4821 363.509073 10.1.0.2 10.1.0.102 IMAP 162 Response: * CAPABILITY IM
4822 363.515890 10.1.0.102 10.1.0.2 IMAP 95 Request: 3 login "sam@515
4823 363.520309 10.1.0.2 10.1.0.1 TCP 66 49750 → 88 [SYN, ECN, CWR
4824 363.520574 10.1.0.1 10.1.0.2 TCP 66 88 → 49750 [SYN, ACK, ECN
4825 363.520591 10.1.0.2 10.1.0.1 TCP 54 49750 → 88 [ACK] Seq=1 Ac
4826 363.520608 10.1.0.2 10.1.0.1 KRB5 277 AS-REQ
4827 363.521861 10.1.0.1 10.1.0.2 KRB5 244 KRB Error: KRB5KDC_ERR_PR
4828 363.521926 10.1.0.2 10.1.0.1 TCP 54 49750 → 88 [FIN, ACK] Seq
Frame 4822: 95 bytes on wire (760 bits), 95 bytes captured (760 bits) on interface 0
Ethernet II, Src: Microsof_01:ca:94 (00:15:5d:01:ca:94), Dst: Microsof_01:ca:92 (00:15:5d:01:ca:92)
Internet Protocol Version 4, Src: 10.1.0.102, Dst: 10.1.0.2
Transmission Control Protocol, Src Port: 1129, Dst Port: 143, Seq: 15, Ack: 124, Len: 41
Internet Message Access Protocol
Line: 3 login "sam@515support.com" "Pa$$w0rd"\r\n
Request Tag: 3
Request Command: login
Request: login "sam@515support.com" "Pa$$w0rd"
0030 02 00 61 06 00 00 33 20 6c 6f 67 69 6e 20 22 73 ··a···3 login "s
0040 61 6d 40 35 31 35 73 75 70 70 6f 72 74 2e 63 6f am@515su pport.co
0050 6d 22 20 22 50 61 24 24 77 30 72 64 22 0d 0a m" "Pa$$ w0rd"··
Remainder of request line (imap.request), 37 bytes
Packets: 59212 · Displayed: 59212 (100.0%)
Profile: Default

Switch Interface Configuration

- Command mode
  - User EXEC
  - Privileged EXEC
  - Configuration modes
- Boot configuration versus running configuration
- Interface status
  - Interface IDs
  - Line status and protocol status
  - Configuration data and traffic statistics
- Autonegotiate speed/duplex versus static config

show config

show interface

MAC Address Table and Port Security

- Database of MAC addresses associated with each port
- Switch floods frames when destination MAC is unknown
- Port security
  - Specify static list of allowed MACs
  - Accept given number of sticky MACs
  - Specify enforcement action for policy violation

show mac address-table

```
NYACCESS1#show mac address-table dynamic
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    000a.8aa2.135e    DYNAMIC     Fa0/23
   1    08cc.683e.fd18    DYNAMIC     Fa0/23
   1    08cc.683e.fd40    DYNAMIC     Fa0/23
   1    18e7.285f.0c28    DYNAMIC     Fa0/24
   1    44ad.d916.2598    DYNAMIC     Fa0/24
   1    5006.04be.159d    DYNAMIC     Fa0/1
Total Mac Addresses for this criterion: 6
```

Port Aggregation

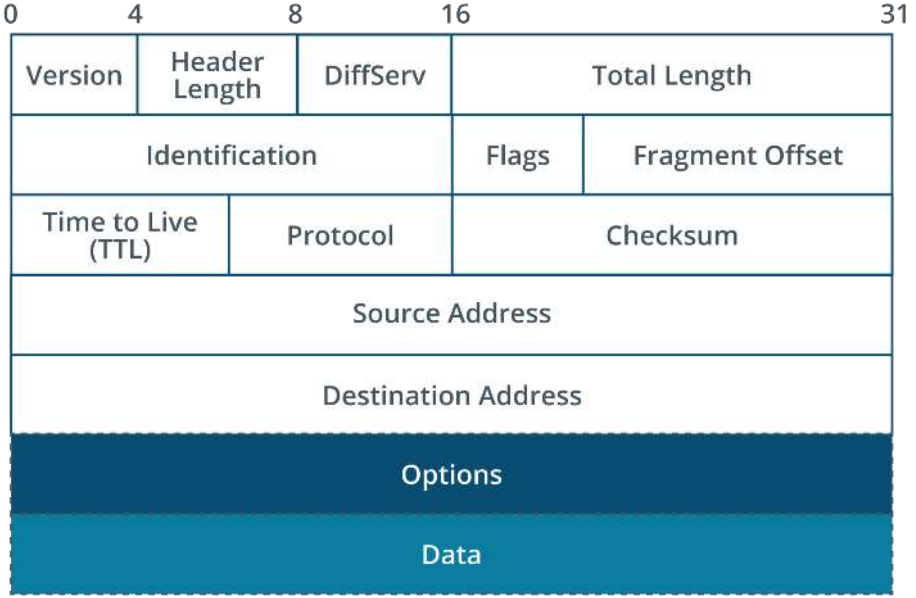
- Combine multiple links into a single logical channel
  - NIC teaming
  - Bonding
- Aggregates link bandwidth
- Provides redundancy
- Link Aggregation Control Protocol (LACP)

Objectives

- Explain IPv4 addressing schemes
- Explain IPv4 forwarding
- Configure IP networks and subnets

IPv4 Datagram Header

- Version
- Length
- Protocol
  - Protocol type in datagram payload
  - Transmission Control Protocol (TCP)
  - User Datagram Protocol (UDP)
  - Internet Control Message Protocol (ICMP)
  - …



IPv4 Address Format (Slide 1 of 2)

- IP address encodes a network ID and a host ID
- 32-bit IPv4

  11000110001010010001000000001001

  - Divide into octets (8 bits)

  11000110 00101001 00010000 00001001

  - Convert each octet to dotted decimal notation

  198.51.100.1

IPv4 Address Format (Slide 2 of 2)

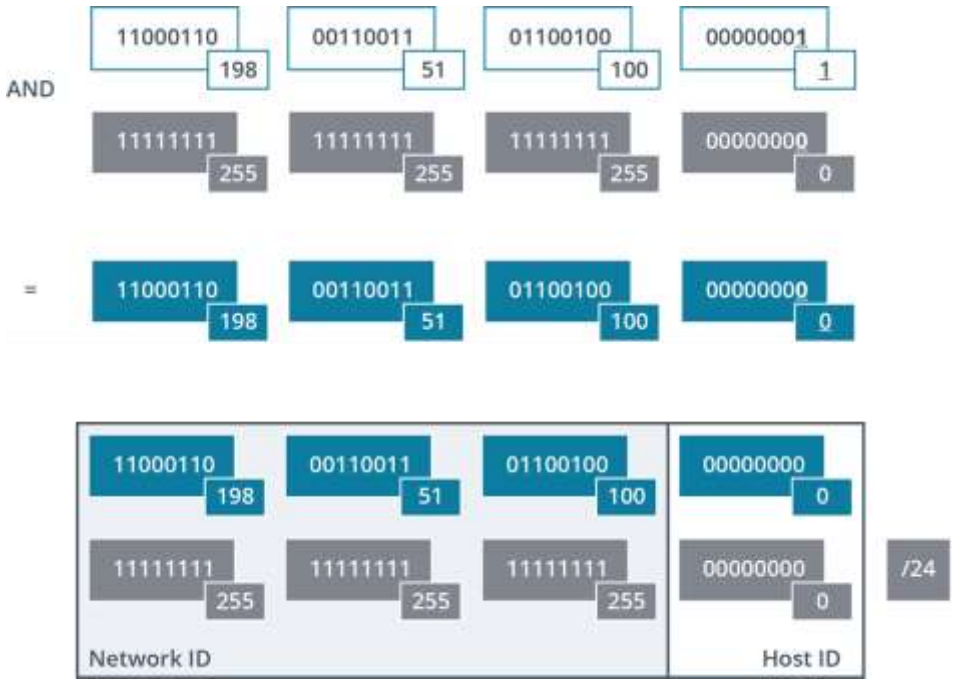
2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	
128	64	32	16	8	4	2	1	
1	1	0	0	0	1	1	0	
128*1	64*1	32*0	16*0	8*0	4*1	2*1	1*0	
128	+64	+0	+0	+0	+4	+2	+0	= 198

	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
	128	64	32	16	8	4	2	1
51 =	0	+0	+32	+16	+0	+0	+2	+1
	0	0	1	1	0	0	1	1

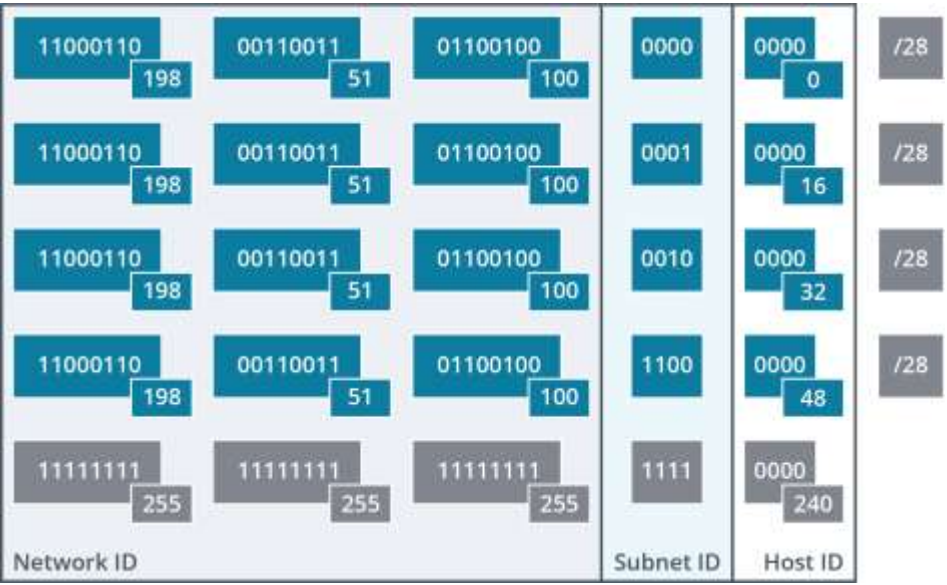
- Binary/decimal conversion
- Range of values from 0.0.0.0 to 255.255.255.255

Network Masks

- Accompanies IP address to reveal network ID part
- Binary 1 in the mask indicates corresponding bit is part of network ID
- Dotted decimal mask or network prefix (slash notation)
- “Default” masks align to octet boundaries



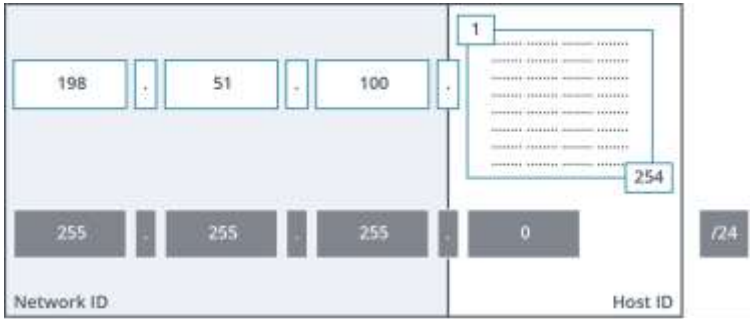
Subnet Masks

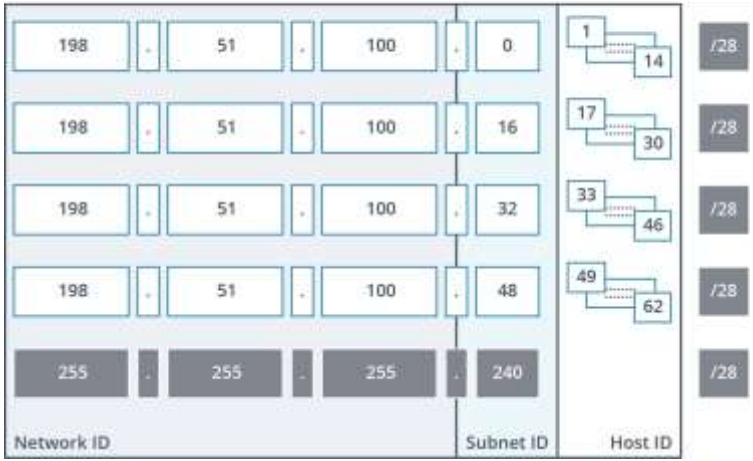


- Divide an IP network into multiple IP subnets
- Designate some host bits as subnet ID bits
- Subnet masks only used within the IP network

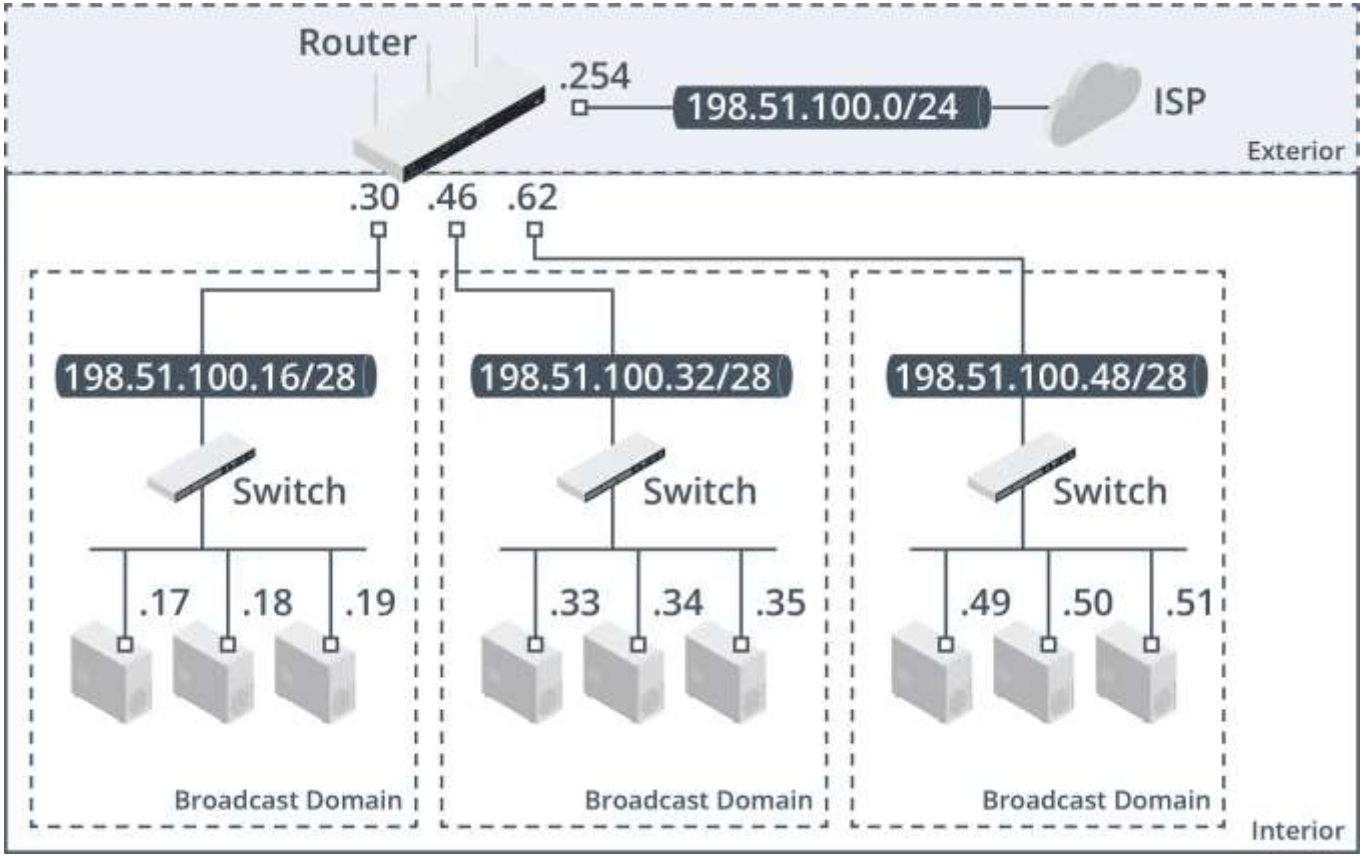
Host Address Ranges

- Number of host bits determines available addresses
  - First address is reserved for the network
  - Last address is reserved for broadcast
- Subnet design fits requirements for number of subnets and hosts per subnet

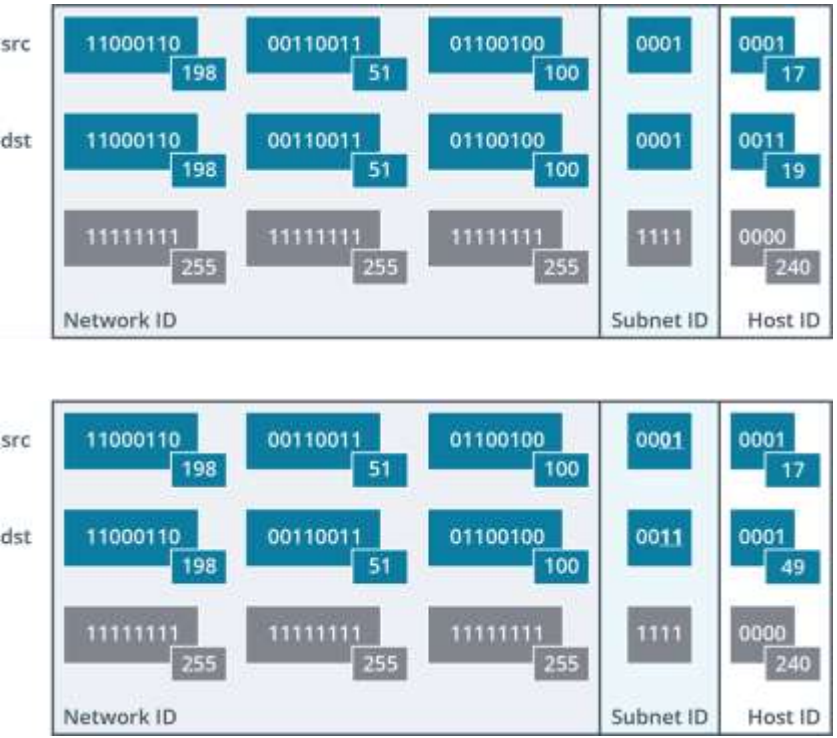




Layer 2 versus Layer 3 Addressing and Forwarding

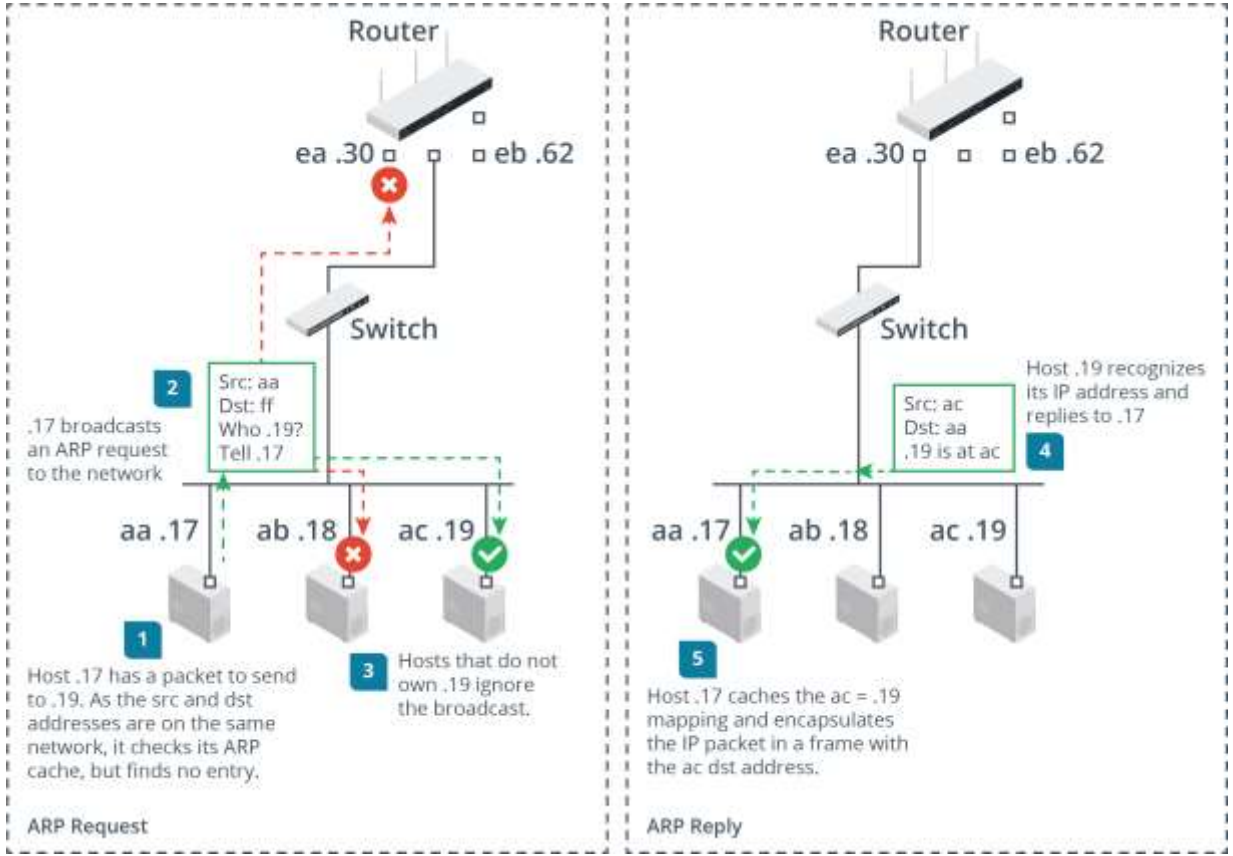


IPv4 Default Gateways



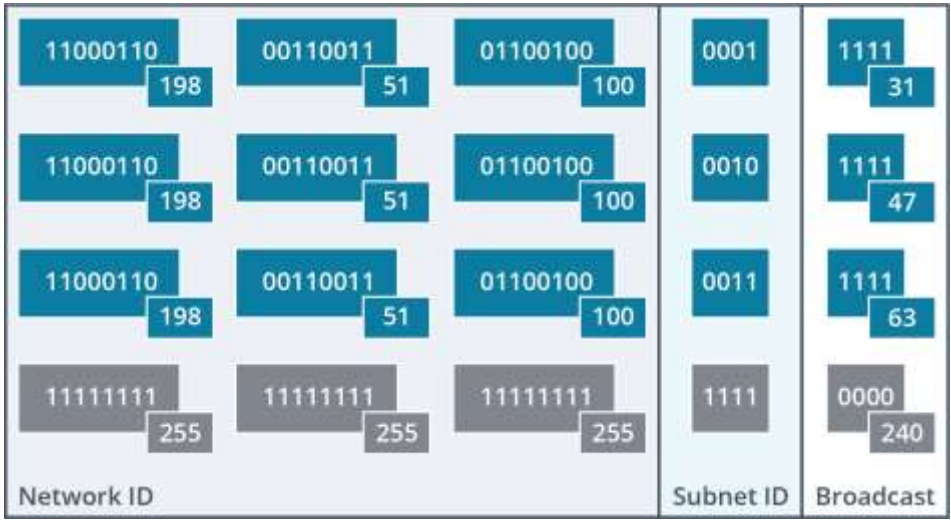
- Compare destination and source addresses against mask
- Local delivery over Ethernet uses Address Resolution Protocol (ARP)
- Remote delivery sent to the default gateway for forwarding
  - Configured as entry in host's local routing table
  - Host uses ARP to locate gateway host on local network
- Default gateway is a router
  - Routers hold paths to multiple networks
  - Paths configured statically or learned using a dynamic routing protocol

Address Resolution Protocol

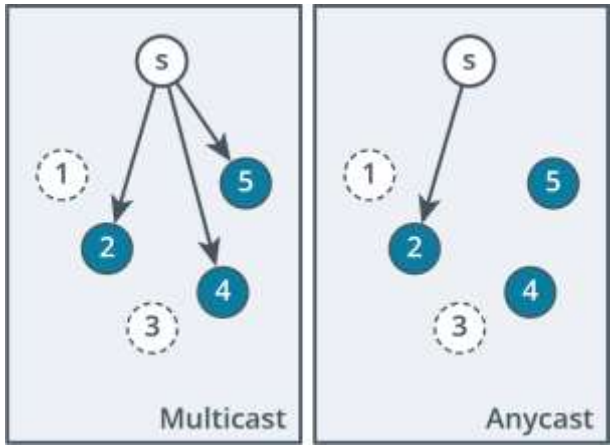


Unicast and Broadcast Addressing

- Unicast packet directed to a single destination IP address
- Broadcast packet directed to all interfaces in the local IP network
  - Layer 3 broadcast domain
  - IP network broadcast address
  - Delivered at layer 2 by broadcast MAC
  - Map layer 3 broadcast domains to layer 2 broadcast domains
  - Routers do not typically forward broadcasts

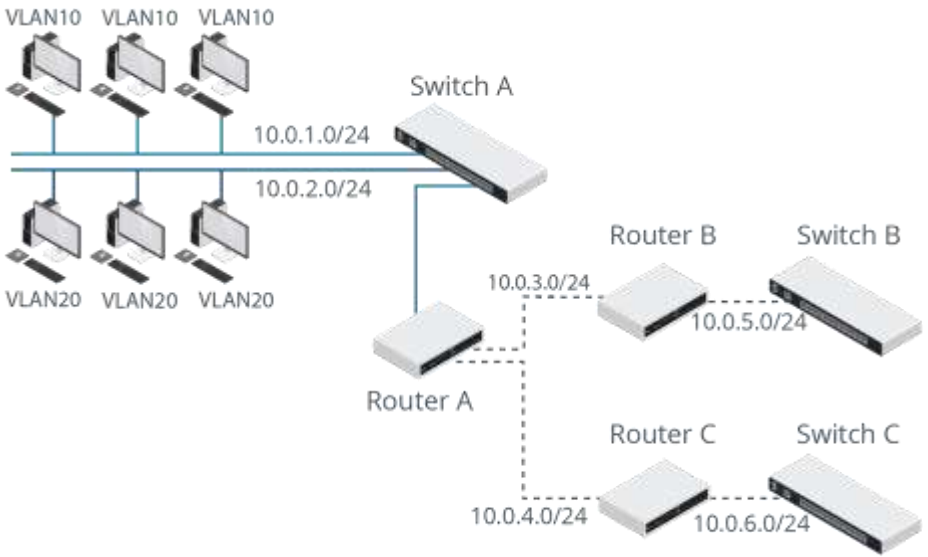


Multicast and Anycast Addressing



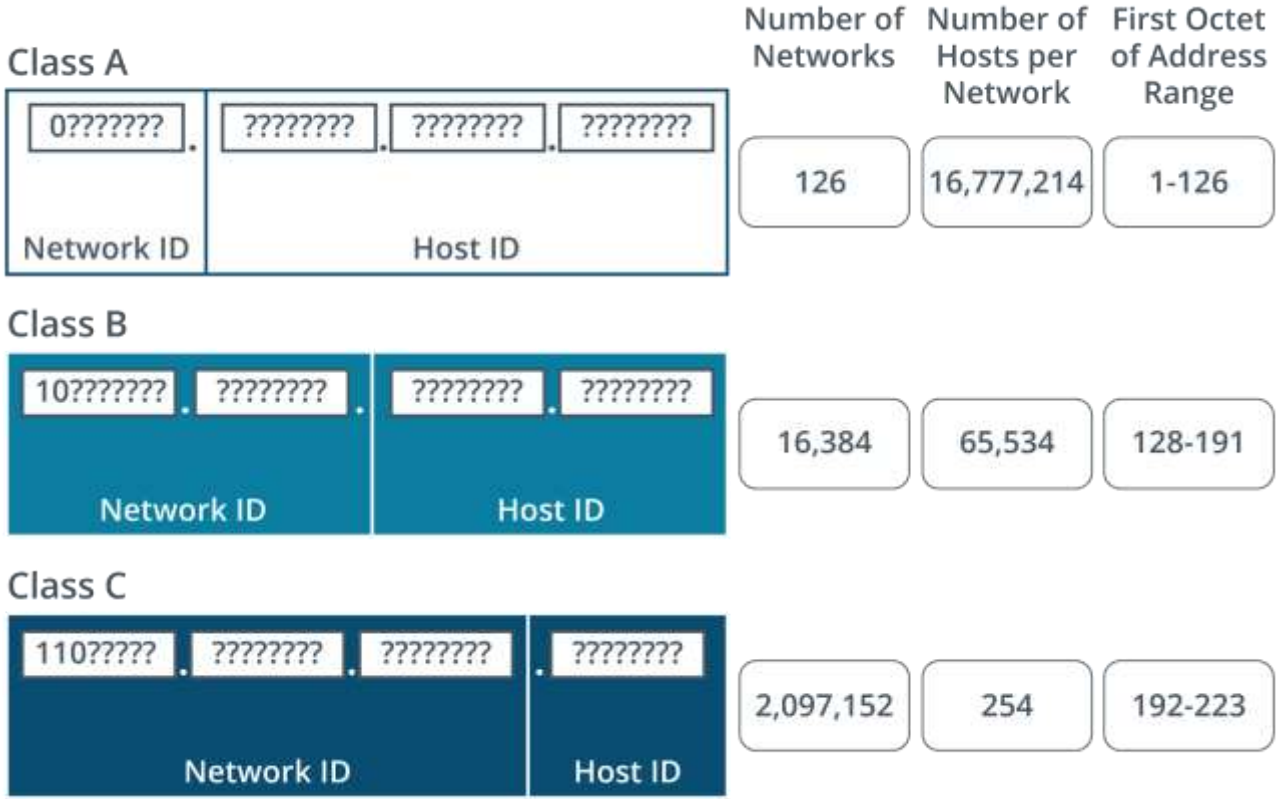
- Multicast
  - Hosts join a multicast group
  - Internet Group Management Protocol (IGMP)
  - IPv4 multicast delivery uses special address ranges
  - Delivery at layer 2
- Anycast
  - Group of hosts configured with same IP address
  - Router forwards to one node only based on prioritization algorithm
  - Used for load balancing and service failover

Virtual LANs and Subnets



- Limit number of hosts within broadcast domain to improve performance
  - Segments identified at layer 3 as subnets
  - Configure virtual LANs (VLANs) on switches to map layer 3 broadcast to layer 2
- Other uses for segmentation
  - Represent WAN links
  - Enforce security zones and boundaries
  - Isolate physical and data link layer segments that use different technologies

Classful Addressing



Public versus Private Addressing

- Public addresses routable over the Internet
  - Governed by IANA and assigned by regional registries and ISPs
- Private address ranges not routable over the Internet
  - 10.0.0.0 to 10.255.255.255
  - 172.16.0.0 to 172.31.255.255
  - 192.168.0.0 to 192.168.255.255
- Hosts on the private network must use some mechanism to access the Internet
  - Network address translation (NAT) or proxy servers
- Automatic Private IP Addressing (APIPA)
  - 169.254.0.0 through 169.254.255.255

Other Reserved Address Ranges

- Class D multicast range
  - 224.0.0.0 through 239.255.255.255
- Class E experimental range
  - 240.0.0.0 through 255.255.255.255
- Loopback range
  - 127.0.0.0 to 127.255.255.255
- Other
  - 0.0.0.0/8 (address unknown)
  - 100.64.0.0/10, 192.0.0.0/24, 192.88.99.0/24, 198.18.0.0/15 (special usage)
  - 192.0.2.0/24, 198.51.100.0/24, 203.0.113.0/24 (documentation and examples)

IPv4 Address Scheme Design (Slide 1 of 2)

- Consider
  - Whether you need a public or private addressing scheme
  - How many networks and subnetworks you need
  - How many hosts per subnet
- Addressing rules
  - Network ID must be from valid range
  - Network and/or host IDs cannot be all 1s or 0s
  - Host ID must be unique in the subnet
- Network ID must be unique
  - On the Internet (in a public addressing scheme)
  - On your internal system of networks (in a private addressing scheme)

IPv4 Address Scheme Design (Slide 2 of 2)

- Calculate how many subnets are needed
  - Round up to nearest power of 2
  - Exponent (the value of n in 2^n) is how many bits to add to the default network prefix
- Check subnets allow sufficient hosts (2^n-2 where n is host bits)
- Calculate the subnets
  - For the first subnet ID, deduct the least significant octet in the mask from 256
  - For the next subnet ID, find the lowest subnet value higher than the previous one
- Calculate the host ranges for each subnet
  - For the first host, add a binary 1 to the subnet address
  - For the last host, deduct two binary digits from the next subnet's ID

Objectives

- Use appropriate tools to test IP configuration
- Troubleshoot IP networks
- Explain IPv6 addressing schemes

IP Interface Configuration

- Configuration parameters
  - IP address and subnet mask
  - Default gateway
  - Domain Name System (DNS) servers
- Manual configuration/static addressing versus autoconfiguration by Dynamic Host Configuration Protocol (DHCP)

ipconfig

- Report network configuration on Windows
  - /all
  - /renew
  - /release
  - /displaydns, /flushdns, /registerdns

```
PS C:\Windows\system32> ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : PC10
   Primary Dns Suffix  . . . . . . . : corp.515support.com
   Node Type . . . . . . . . . . . . : Mixed
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : corp.515support.com

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : corp.515support.com
   Description . . . . . . . . . . . : Microsoft Hyper-V Network Adapter
   Physical Address. . . . . . . . . : 00-15-5D-00-65-31
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : fdf0:2413:6d1c:30:997b:634e:5b90:7e(Preferred)
   Link-local IPv6 Address . . . . . : fe80::997b:634e:5b90:7e%9(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.1.24.101(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Wednesday, August 4, 2021 12:11:31 AM
   Lease Expires . . . . . . . . . . : Thursday, August 12, 2021 12:11:30 AM
   Default Gateway . . . . . . . . . : fe80::215:5dff:fe00:6510%9
                                       10.1.24.254
   DHCP Server . . . . . . . . . . . : 10.1.16.1
   DHCPv6 IAID . . . . . . . . . . . : 67114333
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-27-E6-CC-0C-00-15-5D-00-65-31
   DNS Servers . . . . . . . . . . . : 10.1.16.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
PS C:\Windows\system32>
```

ifconfig and ip

```
lamp@lamp:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.0.201  netmask 255.255.255.0  broadcast 172.16.0.255
        inet6 fe80::215:5dff:fe00:6517  prefixlen 64  scopeid 0x20<link>
        ether 00:15:5d:00:65:17  txqueuelen 1000  (Ethernet)
        RX packets 4042  bytes 589111 (589.1 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 7788  bytes 2885069 (2.8 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 5244  bytes 413133 (413.1 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 5244  bytes 413133 (413.1 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

```
lamp@lamp:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:15:5d:00:65:17 brd ff:ff:ff:ff:ff:ff
    inet 172.16.0.201/24 brd 172.16.0.255 scope global dynamic eth0
       valid_lft 6026sec preferred_lft 6026sec
    inet6 fe80::215:5dff:fe00:6517/64 scope link
       valid_lft forever preferred_lft forever
```

- Linux networking
  - eth0, eth1 or en0, en1
- /etc/network/interfaces
  - ifup and ifdown
- NetworkManager and systemd.networking
- Netplan
- ifconfig (net-tools)
- ip (iproute2)

ARP Cache Utility

- Cache IP:MAC mapping to reduce ARP broadcasts
- arp utility manages cache
  - ip neigh

```
PS C:\Windows\system32> arp -a

Interface: 10.1.24.101 --- 0x9
  Internet Address      Physical Address      Type
  10.1.24.254           00-15-5d-00-65-10     dynamic
  10.1.24.255           ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

Internet Control Message Protocol and ping

```
PS C:\Windows\system32> ping 127.0.0.1 -n 1

Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
PS C:\Windows\system32> ping 10.1.24.101 -n 1

Pinging 10.1.24.101 with 32 bytes of data:
Reply from 10.1.24.101: bytes=32 time<1ms TTL=128

Ping statistics for 10.1.24.101:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
PS C:\Windows\system32> ping 10.1.24.254 -n 1

Pinging 10.1.24.254 with 32 bytes of data:
Reply from 10.1.24.254: bytes=32 time<1ms TTL=64

Ping statistics for 10.1.24.254:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
PS C:\Windows\system32> ping 203.0.113.33 -n 1

Pinging 203.0.113.33 with 32 bytes of data:
Reply from 203.0.113.33: bytes=32 time=2ms TTL=60

Ping statistics for 203.0.113.33:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 2ms, Average = 2ms
```

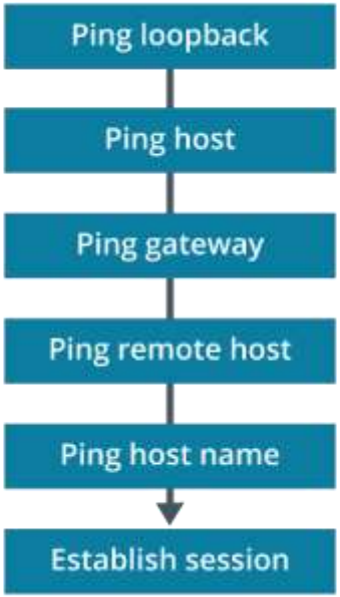
- Report errors and transmit status messaging
- Request and reply packets
  - Time to Live (TTL)
- Destination host unreachable
- No reply (Request timed out)
- Other switches

IP Configuration Issues

- Verify host configuration with ipconfig/ifconfig/ip
- Incorrect IP address
  - Check configuration is consistent with neighbors
- Incorrect subnet mask
  - Host routes traffic that should be delivered locally

Problem Isolation

- ping
  - Loopback
  - Discover neighbors (check ARP cache)
  - Remote host
- Incorrect gateway
  - Check IP of default gateway
  - Check link to default gateway



Incorrect DNS Issues

- Check client’s DNS server address configuration
- Check server availability

IPv6 Address Format

- 128-bit binary address = lots of typing!

  0010 0000 0000 0001 : 0000 1101 1011 1000 : 0000 0000 0000 0000 :
  0000 0000 0000 0000 : 0000 1010 1011 1100 : 0000 0000 0000 0000 :
  1101 1110 1111 0000 : 0001 0010 0011 0100

- Hex notation
  - Each hex digit represents 4 binary digits
  - Arrange hex digits in 8 x 16-bit (double byte) blocks separated by colons

  2001:0db8:0000:0000:0abc:0000:def0:1234

- Canonical notation
  - Omit leading 0s and compress one sequence of all-0 double bytes

  2001:db8::abc:0:def0:1234

IPv6 Network Prefixes

- Host ID is always last 64 bits
- Network prefix (e.g., /48 or /64) determines whether hosts are on same network
- Addressing schemes are different than IPv4
  - Multicast must be supported
  - No broadcasts