Network Health Concept Map

Enterprise Reference Network Print

Produced on
March 25, 2013

Version 5.0

Produced by
Dubberly Design Office
2501 Harrison Street, #7
San Francisco CA, 94110

415 648 9799

Small Office

Small Office network with 256 possible addresses (8 bit)

192.168.1.0/24 (24 bits masked)

Network address	192.168.1.0
Host range from	192.168.1.1
to	192.168.1.254
Broadcast address	192.168.1.255

Small Office User

PCs include ARP tables, routing tables, and firewall rules.

Name	IP Address	MAC Address
Switch	192.168.1.2	5C:09:20:46:AD:R2
Access pt.	192.168.1.3	3D:11:03:27:BC:D1
Phone	192.168.1.105	98:FE:94:23:1D:A0
Printer	192.168.1.106	3C:07:54:47:AD:C3

ARP Table
The smart phone IMEI is governed by other rules, not ARP. Each IP is associated with only one MAC address. If the PC is on both wired and wireless, it will have two IP addresses, one for each connection.

Name	IP Address	Subnet Mask	Route	Weight
Notebook	192.168.1	255.255.255.0	LAN	1
Router	0	0	192.168.1.1	1

Routing Table*
See note below for how to read routing tables.

SRC	SRC IP	DST	DST IP	Port	Time
Any	0	Router	192.168.1.104	80	2300 – 700

Firewall Rules
Specifies what packets to let inside and outside, on which ports, and at what times.

IP Address	Subnet Mask	Route	Weight
10.1.16.0	255.255.240.0	LAN	1
10.1.24.0	255.255.255.0	10.1.24.1	1
0	0	10.1.0.1	1

= I know these devices and can do full packet addressing myself (a.k.a. LAN).
= I don't know the final full address, but I do know what subnet to direct the packets towards at this router.
= I don't know what to do so send packets to next hop (a.k.a. default route).

* **Reading Routing Tables**
The IP Address and Subnet Mask columns identify the source. The zeros signify a wildcard, meaning match any address. (There's not a standard way to identify wildcards, e.g., some manufacturers use an asterisk.)

The route column identifies the destination followed by a weighting factor in terms of how to balance this traffic against any other routes. The lower number wins on the weighting. Weighting is flexible and could be a wide range (e.g., 5, 50, or 500).

Notebook
IP 192.168.1.104
Subnet 255.255.255.0
SRC Port 1104
Ethernet MAC 3C:07:54:47:AD:C1
Wi-Fi MAC 04:54:53:0A:2A:D7
Bluetooth MAC 04:54:53:0A:2A:D8

* Virtual IPs exist if there's a virtual machine running multiple OSs.

Print to wireless printer
SRC 192.168.1.104
DST 192.168.1.106

Each packet of each file that is sent has a source address (SRC) and a destination address (DST). Each device has a different address.

The wireless access point checks its routing table to see if the destination address is inside the its subnet. If it is, the access point routes the packets to the local address. If not, the access point passes the packets on to the next hop.

Smart Phone
IP 192.168.1.105
Subnet 255.255.255.0
SRC Port 1105
IMEI 01 333200 802211 5
Wi-Fi MAC 98:FE:94:23:1D:A0
Bluetooth MAC 98:FE:94:23:1D:A1

Wireless Printer
IP 192.168.1.106
Subnet 255.255.255.0
DST Port 631
Ethernet MAC 3C:07:54:47:AD:C3

802.11n

802.11n

1. Print to wireless printer

Wireless Access Point
IP 192.168.1.3
Subnet 255.255.255.0
Ports 1–4 MAC 3D:11:03:27:BC:D1

hard wired to

Unmanaged switches (OSI layer 2 aware) include an ARP table. Managed switches (OSI layer 3 aware) can include a routing table and DHCP server.

Name	IP Address	MAC Address
Access pt.	192.168.1.3	3D:11:03:27:BC:D1
Notebook	192.168.1.104	04:54:53:0A:2A:D7
Phone	192.168.1.105	98:FE:94:23:1D:A0
Printer	192.168.1.106	3C:07:54:47:AD:C3

ARP Table
The smart phone IMEI is governed by other rules, not ARP. Each IP is associated with only one MAC address. If the PC is on both wired and wireless, it will have two IP addresses, one for each connection.

Switch (optional)
IP 192.168.1.2
Subnet 255.255.255.0
Ports 1–4 MAC 5C:09:20:46:AD:R2
Ports 5–8 MAC 5C:09:20:46:AD:R3

hard wired to

Routers contain a lot of crucial functionality inside which are invisible to end-users. The most important of these many functions are:

Name	IP Address	Subnet Mask	Route	Weight
Router	192.168.1.0	255.255.255.0	LAN	1
ISP	0	0	76.21.40.251	1

Routing Table

SRC	SRC IP	DST	DST IP	Port	Time
Any	0	Router	192.168.1.104	80	2300 – 700

Firewall Rules
Specifies what packets to let inside and outside, on which ports, and at what times.

SRC	SRC LAN IP	SRC Port	DST	DST IP	DST Port
Notebook	192.168.1.104	1004	Gmail	74.125.25.109	80
Phone	192.168.1.105	2010	Gmaps	74.125.224.100	80

Active Conversations Table (a.k.a. Nating Table)
Keeps track of all conversations. Could be up to hundreds at any moment, but 30 on average.

DHCP Server
Dynamically assigns time-leased IP addresses to all connected devices. After expiration, the device requests the same address and is reassigned if the address is still available.

Name	IP Address	MAC Address	Lease
Switch	192.168.1.2	5C:09:20:46:AD:R2	7 days
Access pt.	192.168.1.3	3D:11:03:27:BC:D1	1 day
Notebook	192.168.1.104	04:54:53:0A:2A:D7	8 hours

DHCP Table
Networking problems can occur if the user is in the middle of a process and they are assigned a different IP due to lease expiration. Lease renewal always results in a renewal of the same address.

Diagnostics
Routers have built in diagnostic tools which can be accessed via HTTP in a browser, or via command line interface. Capability varies from model to model, but typically include management of:
- setup
- DHCP
- ports
- firewall
- VPN
- logs

DNS Server
Translate domain names to IP addresses and connect to the world-wide DNS system.

Router (could be wireless)
LAN IP 192.168.1.1
LAN Subnet 255.255.255.0
WAN IP 76.21.40.251
WAN Subnet 255.255.0.0

coax connection provided by contract with ISP

Internet Services

Internet

ISP
Many other routers not shown

ISP Router(s)
WAN IP 76.21.40.1

Router Hops
- block
- neighborhood
- city
- internet backbone router 1, 2, 3...
- internet backbone gateway

Amount of hops depends on physical location and load balancers.

Google

Google Router(s)
WAN IP 72.14.232.136

Router Hops
- Google backbone router 1, 2, 3...
- Google distribution router 1, 2, 3...
- Google Application Data Center router 1, 2, 3...

Amount of hops depends on physical location and load balancers.

Gmail

Incoming SMTP Server
WAN IP 74.125.25.109

IMAP Server
WAN IP 74.125.133.108

Outgoing SMTP Server
WAN IP 74.125.25.109

fiber connection provided by contract with ISP

Enterprise

DMZ (De-Militarized Zone)

Corporate network with 16,777,216 possible addresses (24 bits)

10.0.0.0/8 (8 bits masked)

Network address	10.0.0.0
Host range from	10.0.0.1
to	10.255.255.254
Broadcast address	10.255.255.255

Dedicated Firewall

HTTP Servers
e.g., public website

Incoming SMTP Server

IMAP Server

Outgoing SMTP Server

DNS Server
Translate domain names to IP addresses and connect to the world-wide DNS system.

Core/Backbone

Active/active redundancy (both connections operating) is indicated by blue lines and devices.

Data Center

Core Router 3
WAN IP 76.21.40.200
LAN IP 10.128.0.3
Host range from 10.128.0.1
to 10.191.255.254

Core Router 4
WAN IP 76.21.40.201
LAN IP 10.192.0.4
Host range from 10.192.0.1
to 10.255.255.254

Dedicated Firewall

Router
Connections to additional devices not shown.

Switch
Connections to additional devices not shown.

Load Balancer
May be OSI layer 4–7 aware.

Traffic	Route
33.3%	Server A
33.3%	Server B
33.3%	Server C

Load Balancing Table

Servers

Dedicated Connection

Dedicated Connection

Core Router 1
Host range from 10.1.0.1
to 10.63.255.254

Core Router 2
Host range from 10.64.0.1
to 10.127.255.254

DNS Server
Translate domain names to IP addresses and connect to the world-wide DNS system.

LDAP Server
Enterprise directory of employee contact info and calendars distributed over IP.

Monitoring Server(s)
Pings all devices (via ICMP—echo request/reply). Runs open source Ganglia, HP Open View (SNMP—Simple Network Management Protocol), or Cisco equivalent. Client software runs on all devices to collect data.

Region

MPLS (Multi-protocol Label Switching)
MPLS is a mechanism for directing packets from one node to another based on a short path label, instead of long network addresses which require the CPU to lookup the routing table. The labels identify virtual paths between nodes rather than endpoints.

Label edge routers (LERs) 'push' an MPLS label onto an incoming packet, and 'pop' it off the outgoing packet. Labels are pushed and popped by Label Distribution Protocol (LDP). Labels can be added to other labels, encapsulating the packet and enabling hierarchical routing. MPLS headers do not identify the type of data carried inside the packet (no introspection).

MPLS is independent from the OSI layer model and is generally considered to operate between layers 2 and 3; sometimes referred to as a layer 2.5 protocol. MPLS is eliminates the dependence on a particular technology such as Asynchronous Transfer Mode (ATM), Frame Relay, Synchronous Optical Networking (SONET) or Ethernet.

MPLS

MPLS

AT&T Leased Connection
Routers and switches are leased. There is no visibility into what's going on inside. Devices on either end think they are on the same subnet.

Verizon Leased Connection
Routers and switches are leased. There is no visibility into what's going on inside. Devices on either end think they are on the same subnet.

MPLS

MPLS

California Router 1
IP 10.0.1.1

California Router 2
IP 10.0.1.2

Nevada Router 1
IP 10.16.1.1
Connections to additional devices not shown.

Nevada Router 2
IP 10.16.1.2
Connections to additional devices not shown.

Campus

contains...
San José network with 65,536 possible addresses (16 bits)

10.1.0.0/16 (16 bits masked)

Network address	10.1.0.0
Host range from	10.1.0.1
to	10.1.255.254
Broadcast address	10.1.255.255

San José Router 1 includes firewall rules, active conversations table, and **Routing Table**.

Name	IP Address	Subnet Mask	Route	Weight
SJ 1	10.1.0.0	255.255.0.0	LAN	1
SF 1	10.2.0.0	255.255.0.0	10.2.0.1	1
SF 2	10.2.0.0	255.255.0.0	10.2.0.2	1
Bldg. A 1	10.1.16.0	255.255.240.0	10.1.16.1	1
Bldg. A 2	10.1.16.0	255.255.240.0	10.1.16.2	1
Bldg. B 1	10.1.32.0	255.255.240.0	10.1.32.1	1
Bldg. B 2	10.1.32.0	255.255.240.0	10.1.32.2	1
Cali 1	0	0	10.0.1.1	1
Cali 2	0	0	10.0.1.2	1

4. Print to San Francisco

San José Router 1
LAN IP 10.1.0.1
Subnet 255.255.0.0

San José Router 2
LAN IP 10.1.0.2
Subnet 255.255.0.0

DHCP Server
Dedicated device running Linux. DHCP is not distributed at lower levels.

The site router checks its routing table to see if the destination address is inside the router's subdomain. If it is, the router routes packets to the right subnet. If it's not, the router routes the packets to the next hop.

contains...
San Francisco network with 65,536 possible addresses (16 bits)

10.2.0.0/16 (16 bits masked)

Network address	10.2.0.0
Host range from	10.2.0.1
to	10.2.255.254
Broadcast address	10.2.255.255

San Francisco Router 1 includes firewall rules, active conversations table, and **Routing Table**.

Name	IP Address	Subnet Mask	Route	Weight
SF 1	10.2.0.0	255.255.0.0	LAN	1
SJ 1	10.1.0.0	255.255.0.0	10.1.0.1	1
SJ 2	10.1.0.0	255.255.0.0	10.1.0.2	1
Bldg. A 1	10.1.16.0	255.255.240.0	10.1.16.1	1
Bldg. A 2	10.1.16.0	255.255.240.0	10.1.16.2	1
Bldg. B 1	10.1.32.0	255.255.240.0	10.1.32.1	1
Bldg. B 2	10.1.32.0	255.255.240.0	10.1.32.2	1
Cali 1	0	0	10.0.1.1	1
Cali 2	0	0	10.0.1.2	1

San Francisco Router 1
LAN IP 10.2.0.1
Subnet 255.255.0.0

San Francisco Router 2
LAN IP 10.2.0.2
Subnet 255.255.0.0
Connections to additional devices not shown.

Other site routers function just as the site 1 router does. The site-level routers are linked in a star configuration. Each site router has access to the external internet.

Building

contains...
Building A network with 4,096 possible addresses (12 bits)

10.1.16.0/20 (20 bits masked)

Network address	10.1.16.0
Host range from	10.1.16.1
to	10.1.31.254
Broadcast address	10.1.31.255

3. Print to building B

Building A, Router 1 includes firewall rules, active conversations table, and **Routing Table**.

Name	IP Address	Subnet Mask	Route	Weight
Bldg. A 1	10.1.16.0	255.255.240.0	LAN	1
Wireless	10.1.24.0	255.255.255.0	10.1.24.1	1
SJ 1	0	0	10.1.0.1	1
SJ 2	0	0	10.1.0.2	1

Building A, Router 1
IP 10.1.16.1
Subnet 255.255.240.0

The building router checks its routing table to see if the destination address is inside the router's subdomain. If it is, the router routes packets to the right subnet or switch. If not, the router passes the packets to the next hop.

Building A, Router 2
IP 10.1.16.2
Subnet 255.255.240.0

contains...
Building B network with 4,096 possible addresses (12 bits)

10.1.32.0/20 (20 bits masked)

Network address	10.1.32.0
Host range from	10.1.32.1
to	10.1.47.254
Broadcast address	10.1.47.255

Building B, Router 1 includes firewall rules, active conversations table, and **Routing Table**.

Name	IP Address	Subnet Mask	Route	Weight
Bldg. B 1	10.1.32.0	255.255.240.0	LAN	1
SJ 1	0	0	10.1.0.1	1
SJ 2	0	0	10.1.0.2	1

Building B, Router 1
IP 10.1.32.1
Subnet 255.255.240.0

Building B router functions just as the building A router does. This diagram shows the building A & B routers connected through the main site router. However, the building A router could be connected directly to the building B router, if traffic volume warranted.

Building B, Router 2
IP 10.1.32.2
Subnet 255.255.240.0
Connections to additional devices not shown.

Floor

2. Print to the second floor

This diagram assumes the switches are class 2. More advanced switches have layer 3 functions which make them difficult to distinguish from routers. Class 2 switches do not appear in routing tables but may have an IP for management purposes. One switch may have multiple subnets and multiple VLANs (Virtual Local Area Network).

Floor 1, Switch 1
IP 10.1.16.3
Subnet 255.255.240.0

Floor 1, Switch 2
IP 10.1.16.4
Subnet 255.255.240.0

Floor 2, Switch 1
IP 10.1.16.5
Subnet 255.255.240.0

Floor 2, Switch 2
IP 10.1.16.6
Subnet 255.255.240.0
Connections to additional devices not shown.

Area

category 5 copper cable

Patch panels exist so wiring changes—which can be required often—can be made easily without wearing down the copper connections which are embedded within the walls. Patch panels are essentially cable organizers and do not have any digital presence on the network.

West Patch Panel 1

West Patch Panel 2
Connections to additional devices not shown.

East Patch Panel 1
Connections to additional devices not shown.

East Patch Panel 2
Connections to additional devices not shown.

category 5 copper cable

contains...
Wireless network with 256 possible addresses (8 bits)

10.1.24.0/24 (24 bits masked)

Network address	10.1.24.0
Host range from	10.1.24.1
to	10.1.24.254
Broadcast address	10.1.24.255

Wireless router includes firewall rules, active conversations table, and **Routing Table**.

Name	IP Address	Subnet Mask	Route	Weight
Wireless	10.1.24.0	255.255.255.0	LAN	1
Bldg. A 1	0	0	10.1.16.1	1

Wireless Router
IP 10.1.24.1
Subnet 255.255.255.0

The wireless router checks its routing table to see if the destination address is inside the router's subnet. If it is, the router routes the packet to the local address. If not, the router passes the packets on to the next hop.

1. Print to wireless printer

1 — Print to wireless printer — SRC 10.1.24.101, DST 10.1.24.104
2 — Print to the second floor — SRC 10.1.24.101, DST 10.1.16.101
3 — Print to building B — SRC 10.1.24.101, DST 10.1.32.101
4 — Print to San Francisco — SRC 10.1.24.101, DST 10.2.0.101

Each packet of each file that is sent has a source address (SRC) and a destination address (DST). Each device has a different address.

Desktop
IP 10.1.24.101
Subnet 255.255.255.0
SRC Port 1101
Ethernet MAC A8:20:66:42:87:78
Wi-Fi MAC 8C:2D:AA:37:90:BB
Bluetooth MAC 8C:2D:AA:37:90:BC

Notebook
IP 10.1.24.102
Subnet 255.255.255.0
SRC Port 1102
Ethernet MAC A8:20:66:52:62:30
Wi-Fi MAC 8C:2D:AA:37:90:91
Bluetooth MAC 8C:2D:AA:37:90:92

Smart Phone
IP 10.1.24.103
Subnet 255.255.255.0
SRC Port 1103
IMEI 09 555200 901122 6
Wi-Fi MAC D8:D1:CB:A2:A7:2G
Bluetooth MAC D8:D1:CB:A2:A7:2H

Wireless Printer
IP 10.1.24.104
Subnet 255.255.255.0
DST Port 631
Ethernet MAC A8:20:66:52:67:D3

Floor 2 Printer
IP 10.1.16.101
Subnet 255.255.240.0
DST Port 631
Ethernet MAC 4G:08:55:47:DC:D1

Building B Printer
IP 10.1.32.101
Subnet 255.255.240.0
DST Port 1101
Ethernet MAC 2A:09:33:46:BB:C4

San Francisco Printer
IP 10.2.0.101
Subnet 255.255.0.0
DST Port 1101
Ethernet MAC 2C:11:45:87:2A:D7

Enterprise User

Introduction
This diagram shows two computer networks (a small office network and parts of a large enterprise network) and how they might be connected to the internet. It also shows part of a data center (which might provide any number of services) also connected to the internet.

The purpose of the diagram is to explain computer networks. The reference networks contain examples of most typical device types, their network addresses, and how the devices might be connected. For some devices, key tables (such as routing tables) are shown. All of the computers and routers maintain and use several tables. (Not all tables are shown because of limited space and to avoid undue complication of the diagram.)

Green lines show the flow of packets in a simple network operation (printing a document to printers in different locations). Readers can trace the path of a message through the various routers in the network.

Devices
It's easy to feel overwhelmed when thinking of all the different types of devices on a network. Fortunately, there's a simple way to categorize most devices.

Most devices on the network are computers.
Most switches are computers.
Routers are specialized switches.
Firewalls and load balancers are specialized routers.

Traffic
Networks are used to transfer or send data streams from one computer to another. The process involves exchanging a series of messages comprised of data packets. Each packet carries the address of the source, destination, while the routing table carries the address of the next step (or hop). Devices on the network have several types of addresses.

MAC Addresses (Media Access Control)
A MAC address is a unique fixed identifier (although modern devices enable configuration), which all devices have. Addresses are per communication protocol, not per device. For example, a typical PC has 3 MAC addresses—one for ethernet, one for Wi-Fi, and one for Bluetooth. MAC addresses are used in all network communications at level 2. Every packet contains the MAC address of the next machine in the route. At each machine, the MAC address must be updated for the next machine.

IP Addresses (Internet Protocol)
An IP address is a device identifier that can be changed. Every machine needs an IP address in addition to a MAC address. Some machines will have multiple IP addresses because they act as multiple machines or participate in multiple networks. A router may have an internal IP address and an external IP address. A PC may have one address for each virtual machine or OS.

Every packet contains two IP addresses, one to identify the source and one to identify the destination. They do not change during transmission.

IPv4 address are comprised of 4 octets (numbers from 0 to 255). This address space is large, but not large enough for our growing networks. IPv6 is replacing IPv4 and will use 6 octets creating vastly more addresses. (This diagram describes a network using IPv4.) A number of strategies enable adding more machines without creating new addresses.

There are three classes of IP addresses.
Each class offers a different amount of possibilities.

	Assigned	Unassigned	
Class A	X . X .	X . X	16,777,216 possibilities
Class B	X . X .	X . X	1,048,576 possibilities
Class C	X . X .	X . X	65,536 possibilities

Some IP address are designated private/reserved/non-internet routable (internal). This range of addresses are identified by the first octet. If any of these addresses are found in the public WAN network, the packets are ignored and dropped by the router. Three prefixes are reserved addresses: 10, 172, and 192.

Class A	10.0.0.0	to	10.255.255.255	16,777,216 possibilities
Class B	172.16.0.0	to	172.31.255.255	1,048,576 possibilities
Class C	192.168.0.0	to	192.168.255.255	65,536 possibilities

Subnet Masks
Subnet masks enable network administrators to divide up a range of IP addresses. Similar to a hierarchical tree/folder structure. This organization enables administrators to pinpoint problems and control access.

CIDR notation (Classless Inter-Domain Routing)
A syntax for specifying networks as a single address, instead of using both the IP address and subnet mask. For example, an IP address of 10.1.0.0 with a subnet mask of 255.255.0.0 can be expressed as 10.1.0.0/16. The 16 comes from adding the 8 bits from the first octet and the 8 bits from the second octet. CIDR is usually used to refer to a whole network, not individual devices on the network.

ARP (Address Resolution Protocol)
ARP is a process for translating IP addresses into MAC addresses. Whenever two devices on a network want to connect to each other, the source sends a broadcast packet to the switch that asks the router for the destination device's IP address. The router (typically a switch) then broadcasts to every device connected on the subnet a request that the destination device identify itself. The non-targeted devices ignore the request. When the destination device receives the request, it confirms by sending its MAC and IP addresses back to the router, which sends it back to the source device, and the connection is established.

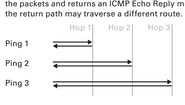
NAT/Natting (Network Address Translation)
Natting is the process of translating the private LAN IP addresses into the public WAN IP address assigned. Unique IP addresses are in short supply so natting enables millions of computers around the world to share the same IP address by their local LAN. This alleviates the need for unique public IP addresses for each LAN device.

Ports
Services communicating over a network are associated with software ports (virtual, not physical). Ports are numbered from 1 to 65,535. 1,000 and below are reserved for servers. 1,000 and above can be used by client applications. Certain ports are commonly assigned to certain types of traffic, e.g., port 80 is always used for HTTP traffic. The port number is key in identifying and routing messages that go through natting. The natting router ensures that port numbers from different private source addresses are not duplicated during the session.

DHCP (Dynamic Host Configuration Protocol)
A server running on routers—typically located within an enterprise office—which dynamically assigns time-leased IP addresses to all devices connected to the router.

Traceroute
A mechanism to determine the path and number of hops required to reach a destination host. Traceroute sends a sequence of ICMP (Internet Control Message Protocol) Echo Request packets to a destination host.

Traceroute works by increasing the TTL (Time To Live) value of each successive set of packets sent. The first set of packets sent have a hop limit value of 1, expecting that they are not forwarded by the first router. The next set have a hop limit value of 2, so that the second router will send the error reply. This continues until the destination host receives the packets and returns an ICMP Echo Reply message. The packets on the return path may traverse a different route.



Lights Out Management (LOM)
Modestly spec'd PC built into (or attached) to servers which enables admins to log in manage remotely. The separate CPU enables the server to remain manageable in the event of a crash.

How to read this map
This map can be dissected into four different layers of visual information.

1. Sections
First are the three main sections: small office, internet services, and enterprise (which is divided into additional sub-sections).

2. Devices + Connections
Next are the devices (and the connections between them). Some devices have blowups which reveal additional internal components. Redundant devices are shown in blue.

3. Subnets
Then the devices are organized into subnets.

4. Network Traffic
Finally network traffic is shown as connections between devices (sometimes spanning different subnets).