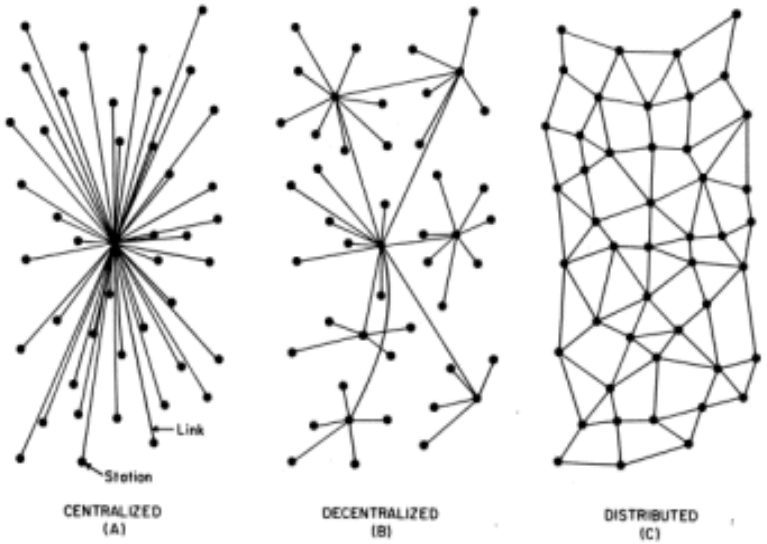
SDSU MASTERS of HOMELAND SECURITY

GEOL600 SENSOR NETWORKS

NETWORK IMPLEMENTATION

The Internet
Local Loop, LAN, MAN, WAN
Cable Modem
Getting Connected
IPv4 IP Addresses
Network Masking
Subnetting
Hubs / Switches
Gateways
Routers
Wireless Routers
Wireless Access Points
Wireless Repeaters
Wireless Bridges
PowerLine Bridges
Power over Ethernet
Network topologies
Product Showcase
Cantenna
Linksys WRT54G router
Linksys WAP54 AP
Dlink 614+ router
Dlink 2100AP
Network example

THE INTERNET

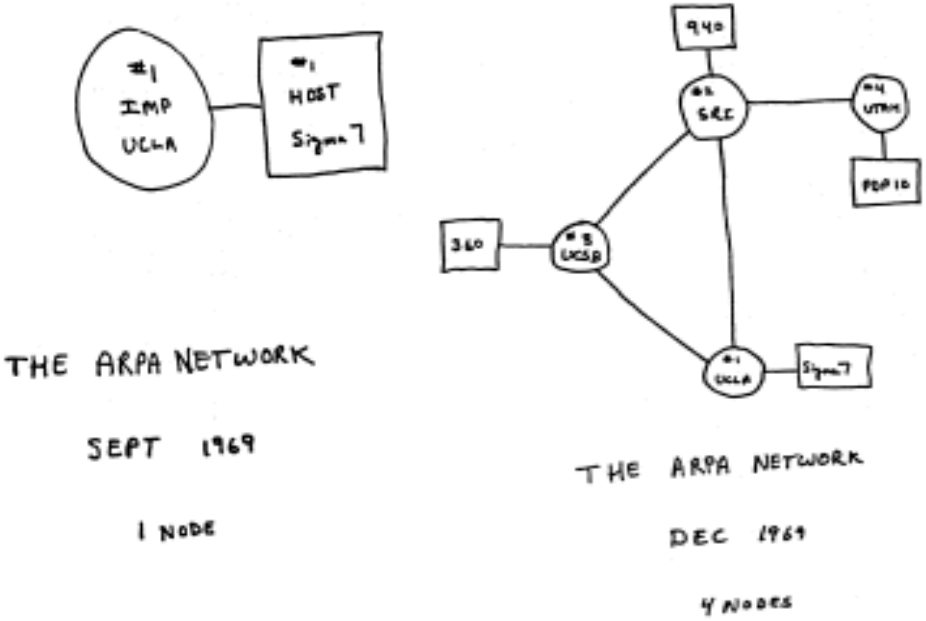


1964

Sketch showing three different network topologies described by Paul Baran in his RAND Memorandum,
"On Distributed Communications: 1. Introduction to DistributedCommunications Network" (August 1964).

In Baran's view the **distributed network** structure offered the **best survivability**.

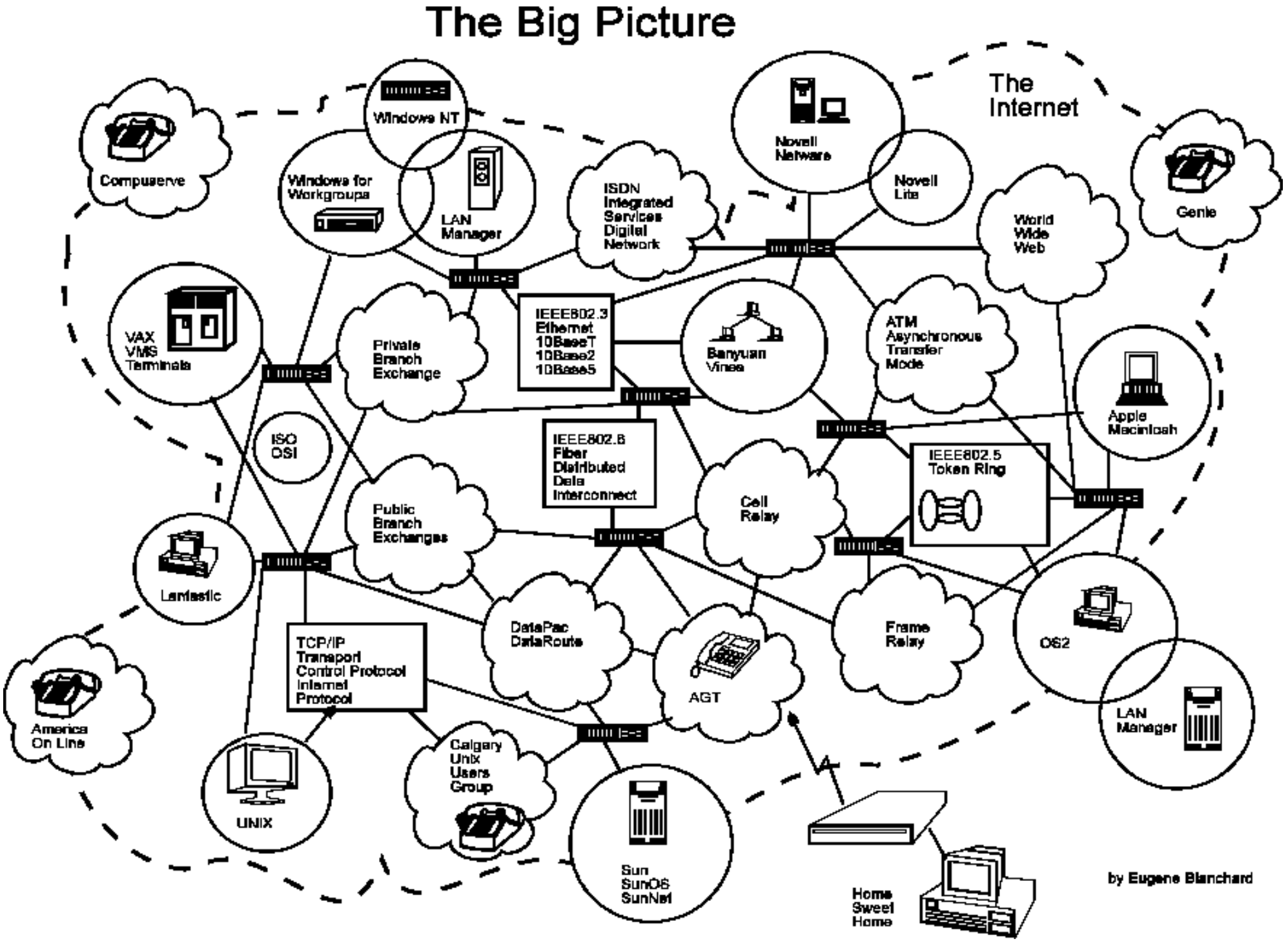
www.rand.org/publications/RM/RM3420/

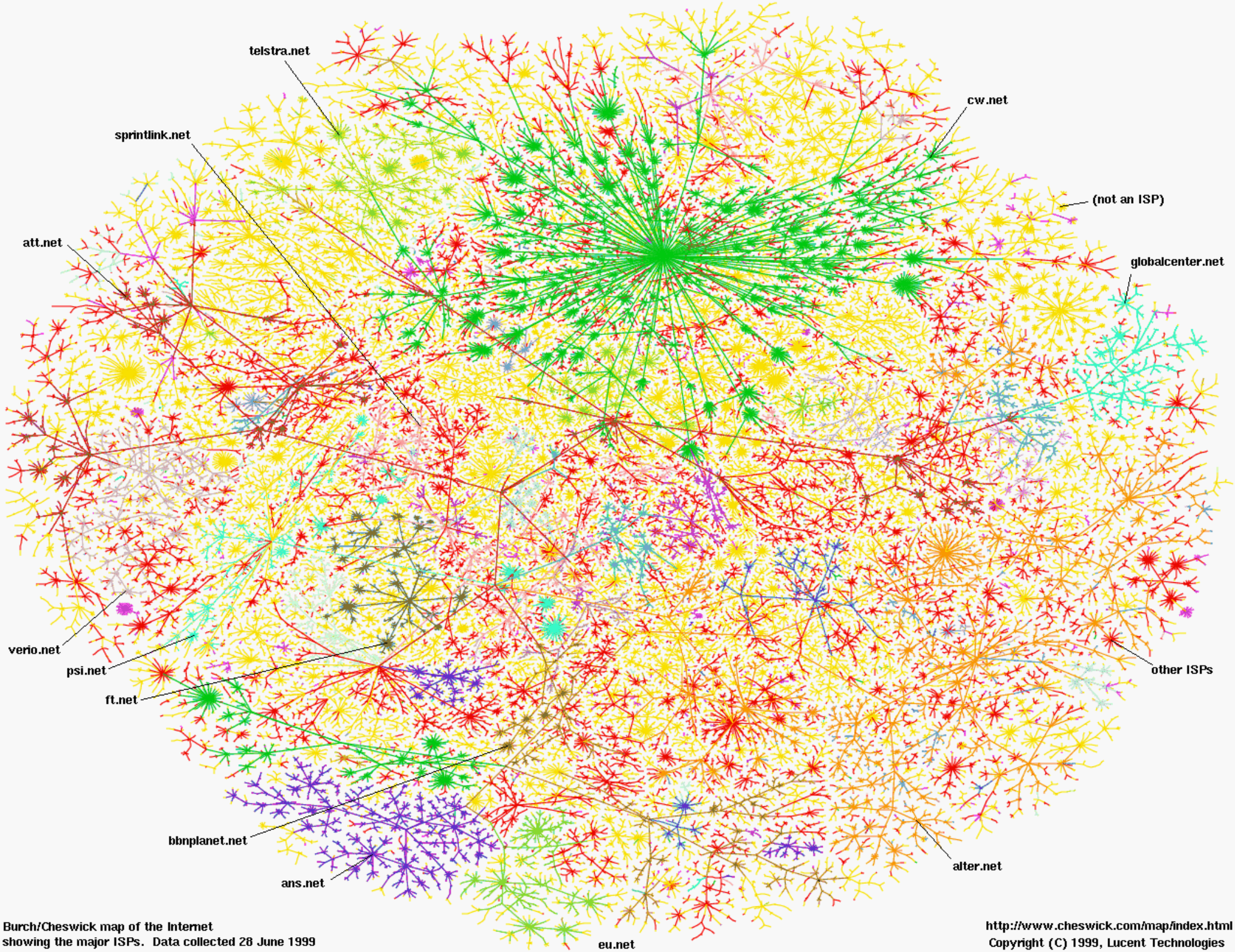


1969

Two sketches from late 1969 of the first nodes on the nascent ARPANET (Advanced Research Project Agency Network) funded by the U.S. Department of Defence.

1999


The Big Picture
The Internet
Compuserve
Windows NT
Windows for Workgroups
LAN Manager
ISDN Integrated Services Digital Network
Novell Netware
Novell Lite
World Wide Web
Genie
VAX VMS Terminals
Private Branch Exchange
IEEE802.3 Ethernet 10BaseT 10Base2 10Base5
Banyuan Vines
ATM Asynchronous Transfer Mode
Apple Macintosh
ISO OSI
IEEE802.6 Fiber Distributed Data Interconnect
IEEE802.5 Token Ring
Cell Relay
Public Branch Exchanges
Lantastic
TCP/IP Transport Control Protocol Internet Protocol
DataPac DataRoute
AGT
Frame Relay
OS2
LAN Manager
America On Line
UNIX
Calgary Unix Users Group
Sun SunOS SunNet
Home Sweet Home
by Eugene Blanchard



Burch/Cheswick map of the Internet
showing the major ISPs. Data collected 28 June 1999

Ref: ATLAS of CYBERSPACES

This is an atlas of maps and graphic representations of the geographies of the new electronic territories of the Internet, the World-Wide Web and other emerging Cyberspaces.

These maps help us visualise and comprehend the new digital landscapes beyond our computer screen, in the wires of the global communications networks and vast online information resources. The cybermaps, like maps of the real-world, help us navigate the new information landscapes, as well being objects of aesthetic interest. They have been created by 'cyber-explorers' of many different disciplines, and from all corners of the world.

www.cybergeography.org/atlas/atlas.html

auths:
Martin Dodge & Rob Kitchin

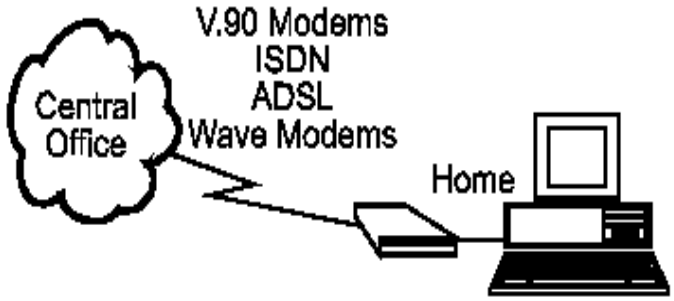
LOCAL LOOP, LAN, MAN, WAN

LOCAL LOOP

often called "the last mile", it refers to the last mile of analog phone line that goes from the telephone company's central office (CO) to your house. Typical local loop protocols are:

- Modem connections - 56 kbps
- ISDN (Integrated Services Digital Network)
  2 x 64 kbps digital lines
- ADSL (Asymmetrical Digital Subscriber Line)
  up to 8 Mbps
- Cable Modems - up to 30 Mbps

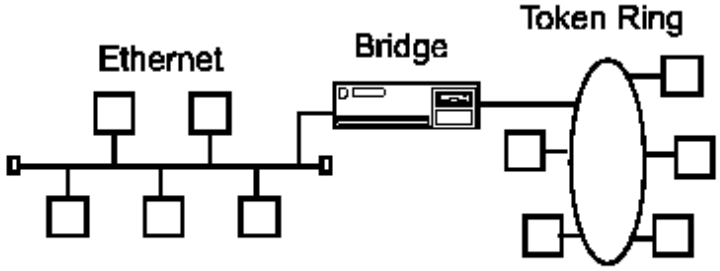
Note: Cable modems are not part of the local loop but do fall into the category of the last mile, or how high speed digital communication gets to the premises (home).



The Local Loop (Last Mile)

LAN (local area networks)
connect computers and resources together in a building or buildings that are close together

Usually have distributed processing, which means that there are many desktop computers distributed around the network and that there is no central processor machine (mainframe).

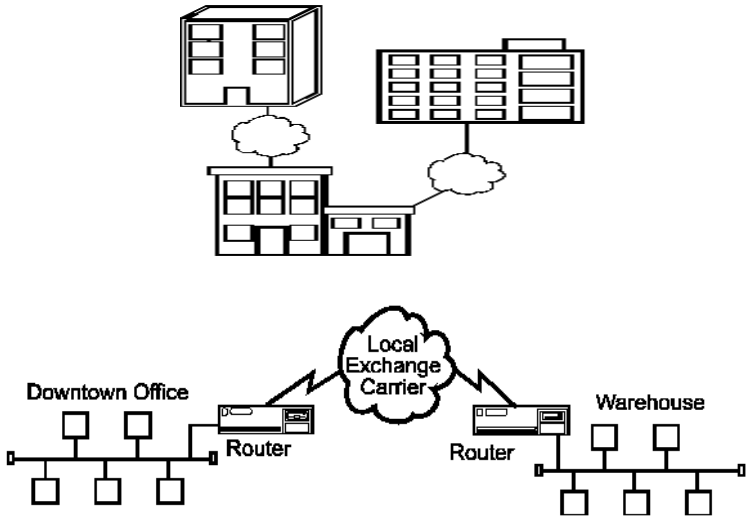


Local Area Network in a building

MAN

Metropolitan Area Networks connect LANs together within a city or metropolitan area.

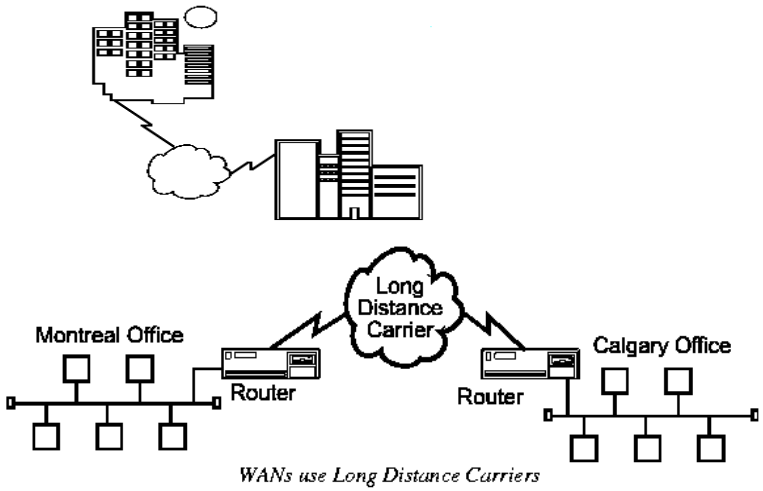
Branch offices are connected to head offices through MANs. Examples of organizations that use MANs are universities and colleges, grocery chains, and banks.



MANs use Local Exchange Carriers

WAN

Wide Area Networks connect LANs together between cities, countries, or continents together. WANs are connected together using one of the telecommunications media.



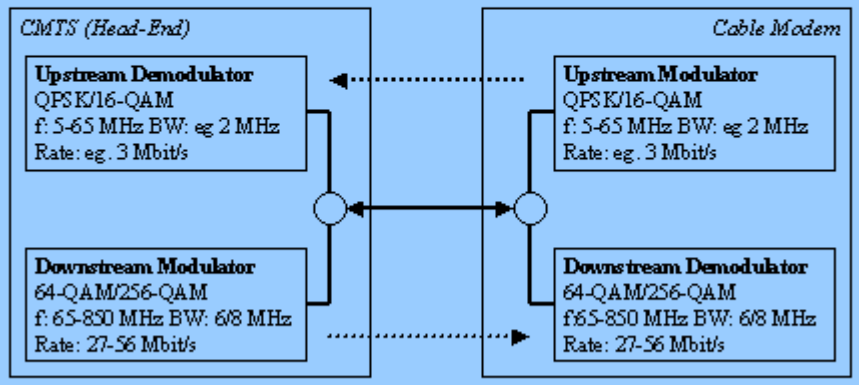
WANs use Long Distance Carriers

https://secure.linuxports.com/howto/intro_to_networking/book1.htm

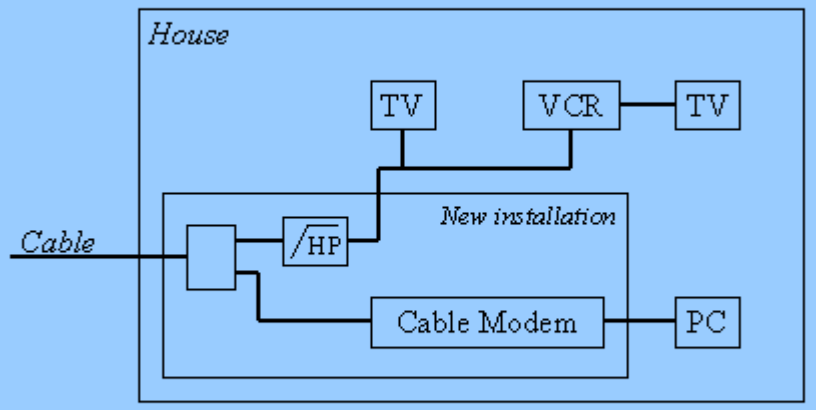
CABLE MODEM

What does Cable Modem mean?

- "CABLE" is short for Cable TV (CATV) Network
- "MODEM" is **MO**dulator-**DEM**odulator
- Actually more like a network adapter than a modem



Typical Cable Modem Installation

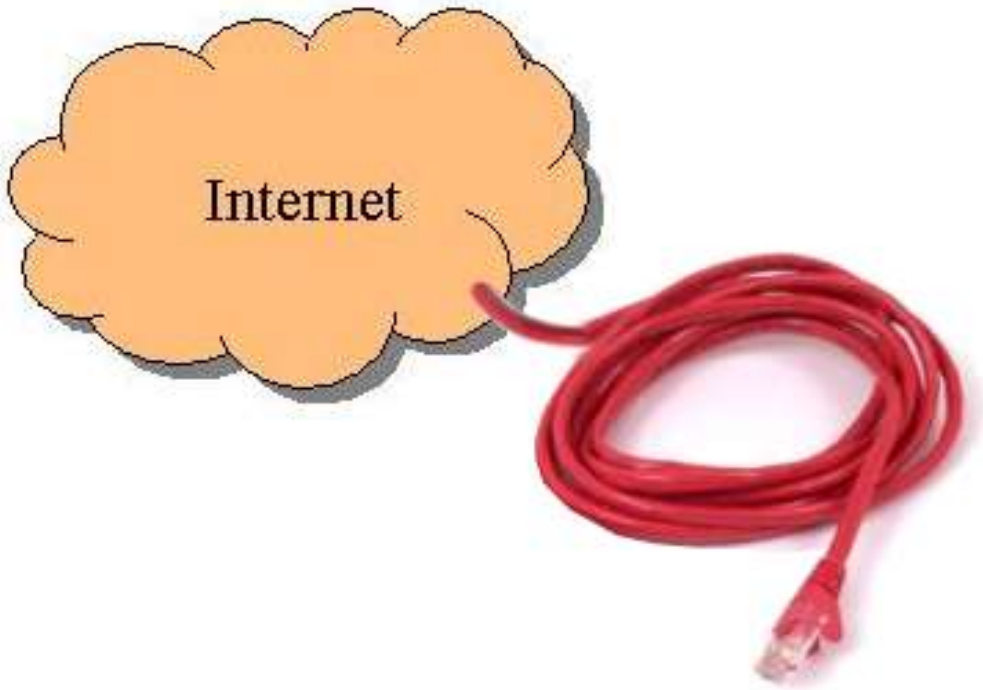


Cable Modem refers to a modem that operates over the ordinary cable TV network cables. Basically you just connect the Cable Modem to the TV outlet for your cable TV, and the cable TV operator connects a Cable Modem Termination System (CMTS) in his end (the Head-End).

Actually the term "Cable Modem" is a bit misleading, as a Cable Modem works more like a Local Area Network (LAN) interface than as a modem.

www.cable-modems.org/tutorial/index.htm

GETTING CONNECTED



Assuming that the backbone connection is in place, for all intents, we are presented with either a live RJ45 cable or a live wall socket.

Our task is to rapidly deploy a network of wired and wireless nodes using this infrastructure.

IPv4 IP ADDRESSES

IP addresses consist of a 32-bit number, and is represented by the dot-decimal format. There are 4 decimal digits separated by three dots. Each digit is allowed the range of 0 to 255.

A portion of an IP address represents the network address, and the remaining portion the host address. Each host on the network--and Internet--must have a unique IP address. There are ways around having each host a unique IP address.

Example:
192.110.237.1 is the IP address of a router.
The network that the router resides on is **192.110.237.0**
The host address of the router is **0.0.0.1**

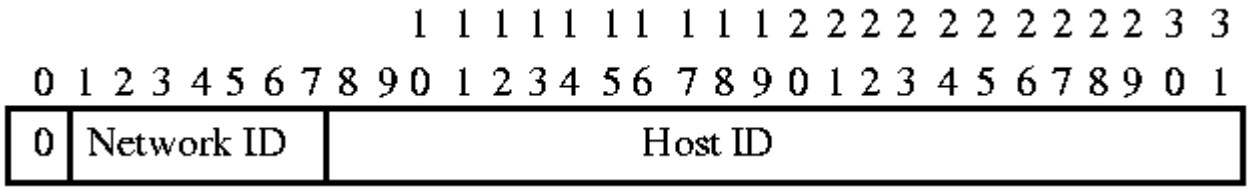
The Network Information Center (NIC) assigns network addresses to the Internet. You must apply to receive a IP network address. Depending on the class of the IP address, you can then assign as many host IP addresses as are allowed.

IP ADDRESS CLASSIFICATIONS

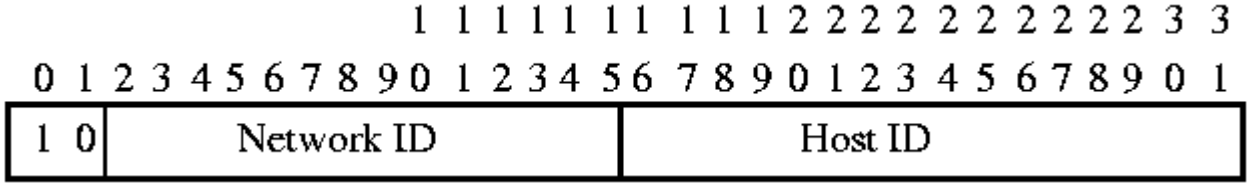
There is a formal structure to the assignment of IP addresses.

There are several classifications of IP addresses: they include network addresses and special purpose addresses.

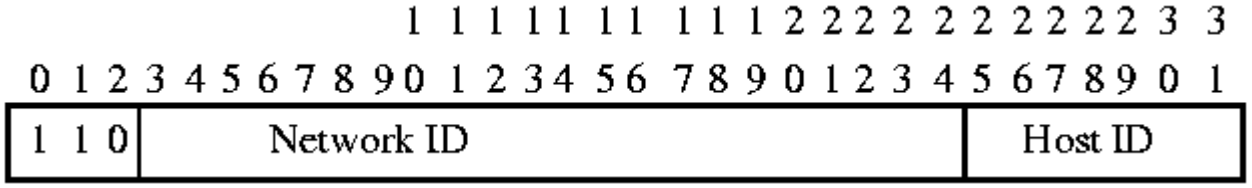
Class A



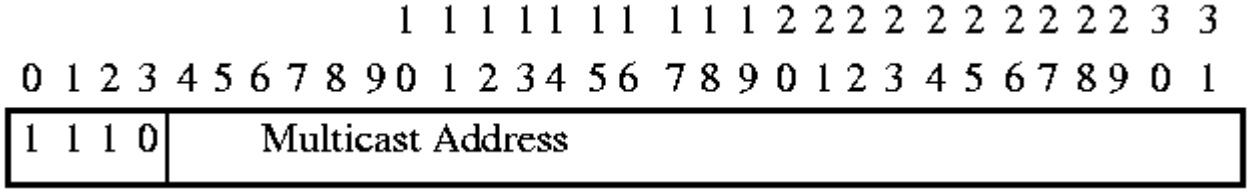
Class B



Class C



Class D



Class A addresses

IP range **1.0.0.0 – 127.0.0.0** Net Mask:**255.0.0.0**
Special Addresses:

10.0.0.1 to **10.255.255.254** for networks not connected to the Internet

127.0.0.1 is the loopback address for testing (see ping)

Number of networks available:125

Number of hosts per network:16,777,214

Class A addresses always have bit 0 set to 0;
bits 1-7 are used as the network ID; bits 8-31 are used as the host ID.
Class A networks are used by very large companies, such as IBM, DoD and AT&T.

Class B addresses

IP range **128.0.0.0 – 191.255.255.255** Net Mask:**255.255.0.0**

Special Addresses:
172.16.0.1 to **172.31.255.254** for networks not connected to the Internet

Number of networks available:16,382

Number of hosts per network:65,534
Class B addresses always have bit 0 and 1 set to 10.
Bits 2-15 are used as the network ID. Bits 16-31 are used as the host ID.
Class B networks are assigned to large companies and universities.

Class C addresses

IP range **192.0.0.0 - 223.255.255.255** Net Mask:**255.255.255.0**

Special Addresses:
192.168.0.1 to **192.168.255.254** for networks not connected to the Internet

Number of networks available: 2,097,150

Number of hosts per network: 254

Class C addresses always have bits 0-2 set to 110.
Bits 3-24 are used as the network ID. Bits 25-31 are used as the host ID.
Class C network addresses are assigned to small companies and local ISPs.

Class D Addresses

IP range **224.0.0.0** to **239.255.255.255**
Use:Multicasting addresses

Class D addresses always have bits 0-3 set to 1110,
bits 4-31 are used as the Multicast address.

Multicasting is a method of reducing network traffic (rather than send a separate datagram to each host if multiple host require the same information). A special multicast address can be used where one datagram is read by many hosts.

Class E Addresses

IP addresses range from **240.0.0.0** to **255.255.255.255**

Use: Reserved by the Internet for its own use.

BROADCAST ADDRESS

A special type of IP address is the limited broadcast address 255.255.255.255. A broadcast involves delivering a message from one sender to many recipients. Senders direct an IP broadcast to 255.255.255.255 to indicate all other nodes on the local network (LAN) should pick up that message. This broadcast is 'limited' in that it does not reach every node on the Internet, only nodes on the LAN.

Technically, IP reserves the entire range of addresses from 255.0.0.0 through 255.255.255.255 for broadcast, and this range should not be considered part of the normal Class E range.

PRIVATE NON ROUTABLE ADDRESS

The IP standard defines specific address ranges within Class A, Class B, and Class C reserved for use by private networks (intranets).

Nodes are effectively free to use addresses in the private ranges if they are not connected to the Internet, or if they reside behind firewalls or other gateways that use Network Address Translation (NAT).

Class	Private start address	Private finish address
A	10.0.0.0	10.255.255.255
B	172.16.0.0	172.31.255.255
C	192.168.0.0	192.168.255.255

NETWORK MASKING

The subnet mask is used to determine which portion of the IP address is the network address, and which is the host address. This means that the portions of network to host in an IP address can change.
The most common subnet mask is 255.255.255.0.

A simple explanation is that wherever there is a 255, this indicates that it is the network portion. Wherever there is a 0, this indicates the host portion.

Example:

if host **192.110.237.1** wants to send a datagram to **192.110.237.21**,
it would look at the network portion of the destination IP address and determine that it is on the local network and send out the datagram.

if host **192.110.237.1** wants to send a datagram to **192.110.150.108**,
it determines that destination is not on the same network, but on 192.110.150.0 and it would send the datagram to the default gateway, a router that knows how to reach the other networks.

A network address becomes a reserved address that should not be assigned to any actual host. Configuring a live host to use the network address could impact communications for all hosts on that network.

Class	Host address range	Network address	Default mask
A	1.0.0.0 - 127.255.255.255	**x**.0.0.0	255.0.0.0
B	128.0.0.0 - 191.255.255.255	**x.x**.0.0	255.255.0.0
C	192.0.0.0 - 223.255.255.255	**x.x.x**.0	255.255.255.0

CLASS MASKING

Class A, B and C networks use masks, not subnet masks. Masks are similar to subnet masks, except that they are normally used in routers (not workstations).

Class A network mask of 255.0.0.0, allows approx. 16.7 million host addresses.
Class B network mask of 255.255.0.0, allows approx 65,00 host addresses.

Both classes of networks have too many hosts for one network to handle.
Imagine 65,000 users trying to access a network service at the same time.
The network would be swamped with requests, and would slow down to a crawl.

The solution is to divide the network up into smaller workable networks, called subnets. This is usually done by fooling the host machine into believing that it is on a Class C network (only 254 hosts). The "fooling" occurs by using a Class C mask 255.255.255.0, called the subnet mask.

Thus, for a Class A network using a subnet mask of 255.255.255.0,
you can have roughly 65 thousand subnets (of 254 hosts).

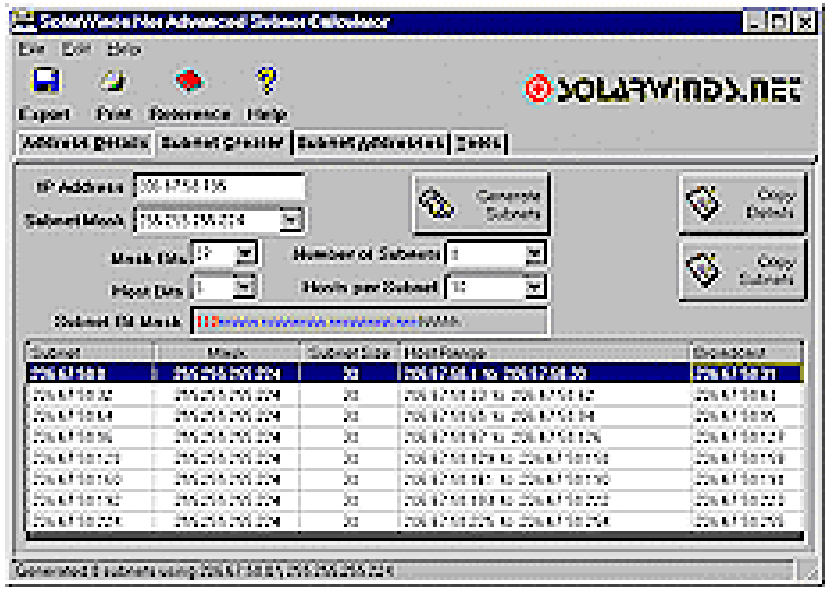
On a Class B network, using a subnet mask of 255.255.255.0,
you can have roughly 254 subnets of 254 hosts.

SUBNETTING

Subnetting allows network administrators some flexibility in defining relationships among network hosts. Hosts on different subnets can only "talk" to each other through specialized network gateway devices like routers. The ability to filter traffic between subnets can make more bandwidth available to applications and can limit access in desirable ways.

Subnet masks can divide networks into smaller networks (< 254 hosts). Subnetting is essentially the modification of a single IP network to create two or more logically visible sub-sections. It entails changing the subnet mask of the local network number to produce an even number of smaller network numbers, each with a corresponding range of IP addresses.

Advanced Subnet Calculator

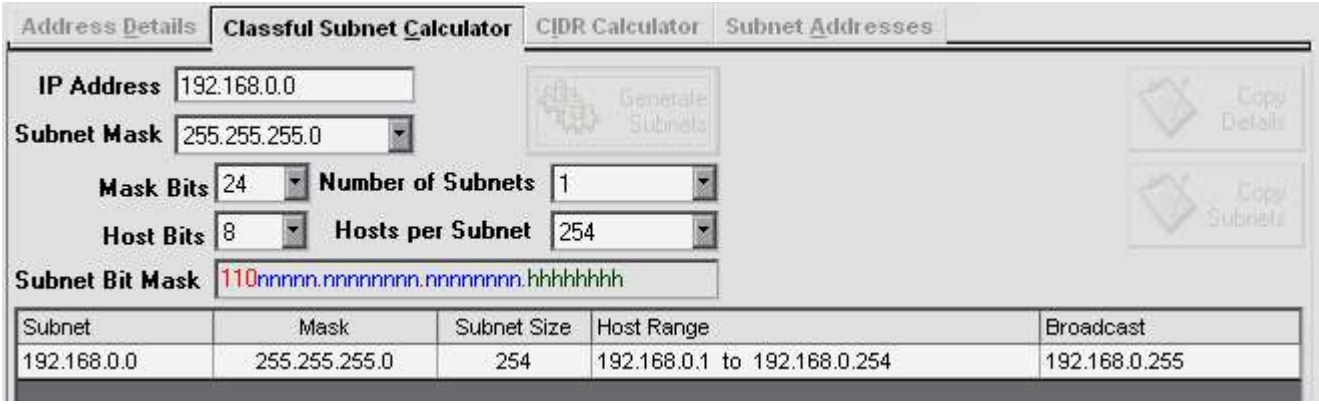


Advanced Subnet Calculator provides comprehensive Subnet Calculator and also performs CIDR (Classless Inter-Domain Routing). In addition to this it performs full DNS resolution and even provides a list of addresses generated which can be exported and used as a working document.

(FREEWARE)

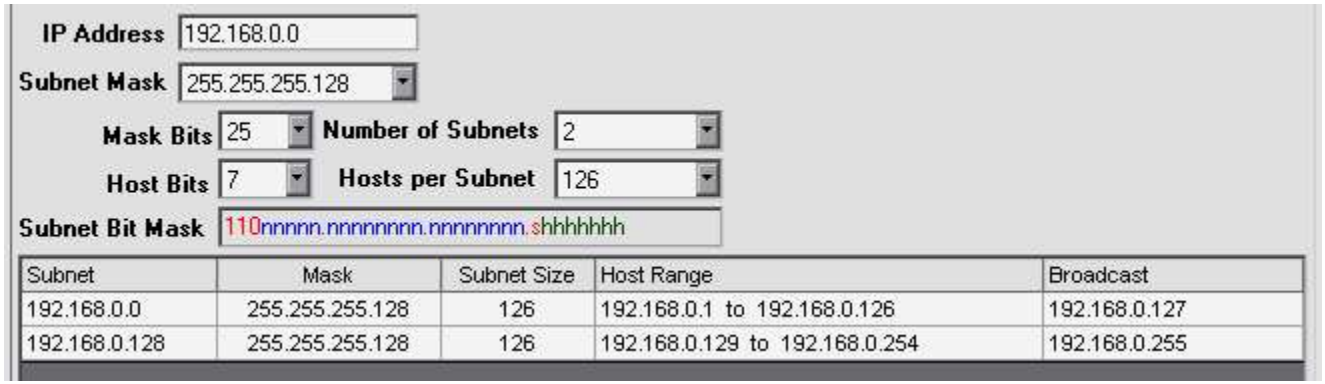
http://support.solarwinds.net/updates/SelectProgramFree.cfm

192.168.0.0/24
1 subnet
254 hosts



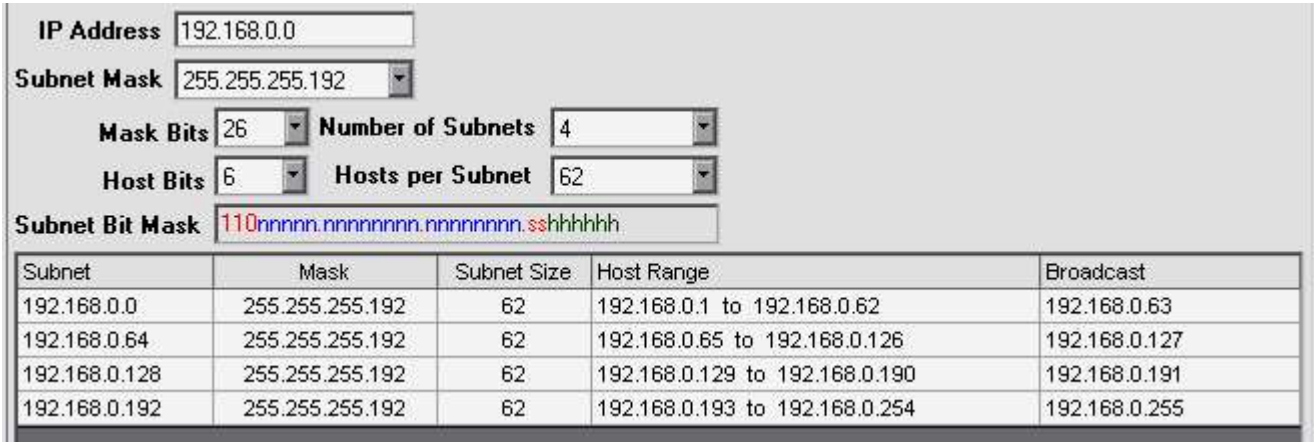
Subnet	Mask	Subnet Size	Host Range	Broadcast
192.168.0.0	255.255.255.0	254	192.168.0.1 to 192.168.0.254	192.168.0.255

192.168.0.0/25
2 subnets
126 hosts



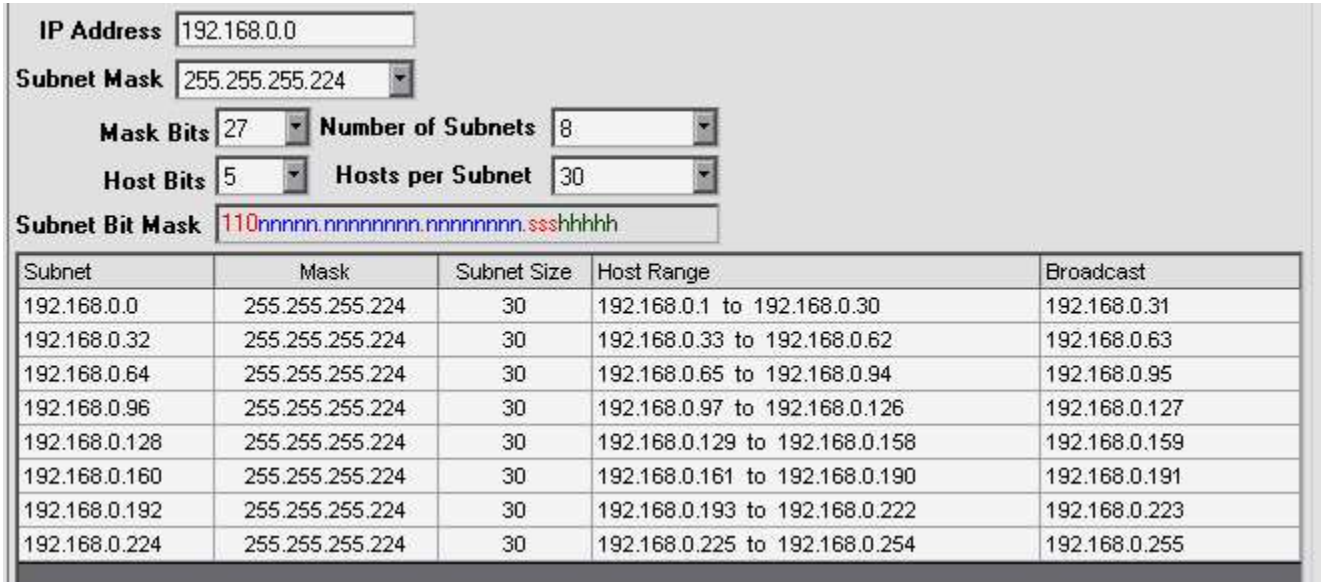
Subnet	Mask	Subnet Size	Host Range	Broadcast
192.168.0.0	255.255.255.128	126	192.168.0.1 to 192.168.0.126	192.168.0.127
192.168.0.128	255.255.255.128	126	192.168.0.129 to 192.168.0.254	192.168.0.255

192.168.0.0/26
4 subnets
62 hosts



Subnet	Mask	Subnet Size	Host Range	Broadcast
192.168.0.0	255.255.255.192	62	192.168.0.1 to 192.168.0.62	192.168.0.63
192.168.0.64	255.255.255.192	62	192.168.0.65 to 192.168.0.126	192.168.0.127
192.168.0.128	255.255.255.192	62	192.168.0.129 to 192.168.0.190	192.168.0.191
192.168.0.192	255.255.255.192	62	192.168.0.193 to 192.168.0.254	192.168.0.255

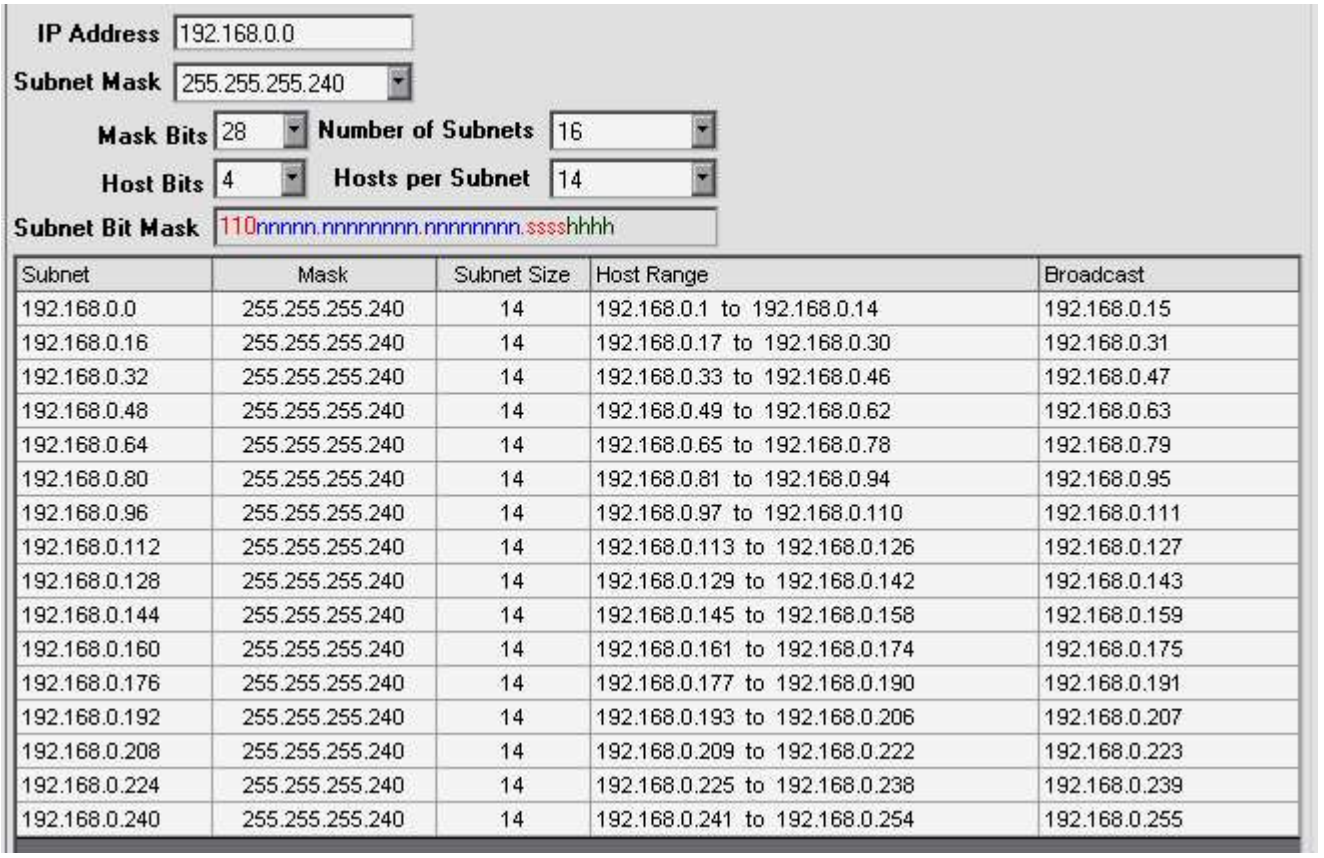
192.168.0.0/27
8 subnets
30 hosts



IP Address: 192.168.0.0
Subnet Mask: 255.255.255.224
Mask Bits: 27 Number of Subnets: 8
Host Bits: 5 Hosts per Subnet: 30
Subnet Bit Mask: 110nnnnn.nnnnnnnn.nnnnnnnn.sssshhhh

Subnet	Mask	Subnet Size	Host Range	Broadcast
192.168.0.0	255.255.255.224	30	192.168.0.1 to 192.168.0.30	192.168.0.31
192.168.0.32	255.255.255.224	30	192.168.0.33 to 192.168.0.62	192.168.0.63
192.168.0.64	255.255.255.224	30	192.168.0.65 to 192.168.0.94	192.168.0.95
192.168.0.96	255.255.255.224	30	192.168.0.97 to 192.168.0.126	192.168.0.127
192.168.0.128	255.255.255.224	30	192.168.0.129 to 192.168.0.158	192.168.0.159
192.168.0.160	255.255.255.224	30	192.168.0.161 to 192.168.0.190	192.168.0.191
192.168.0.192	255.255.255.224	30	192.168.0.193 to 192.168.0.222	192.168.0.223
192.168.0.224	255.255.255.224	30	192.168.0.225 to 192.168.0.254	192.168.0.255

192.168.0.0/28
16 subnets
14 hosts



IP Address: 192.168.0.0
Subnet Mask: 255.255.255.240
Mask Bits: 28 Number of Subnets: 16
Host Bits: 4 Hosts per Subnet: 14
Subnet Bit Mask: 110nnnnn.nnnnnnnn.nnnnnnnn.ssssHHHH

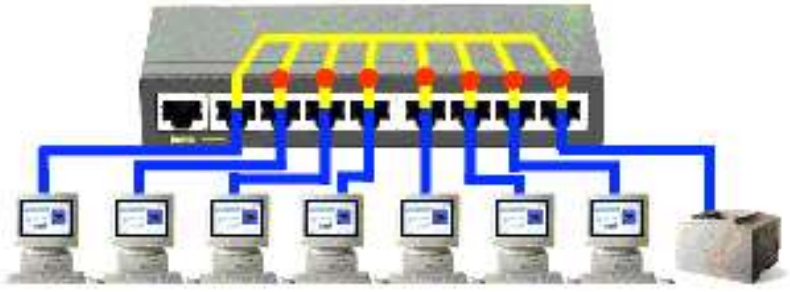
Subnet	Mask	Subnet Size	Host Range	Broadcast
192.168.0.0	255.255.255.240	14	192.168.0.1 to 192.168.0.14	192.168.0.15
192.168.0.16	255.255.255.240	14	192.168.0.17 to 192.168.0.30	192.168.0.31
192.168.0.32	255.255.255.240	14	192.168.0.33 to 192.168.0.46	192.168.0.47
192.168.0.48	255.255.255.240	14	192.168.0.49 to 192.168.0.62	192.168.0.63
192.168.0.64	255.255.255.240	14	192.168.0.65 to 192.168.0.78	192.168.0.79
192.168.0.80	255.255.255.240	14	192.168.0.81 to 192.168.0.94	192.168.0.95
192.168.0.96	255.255.255.240	14	192.168.0.97 to 192.168.0.110	192.168.0.111
192.168.0.112	255.255.255.240	14	192.168.0.113 to 192.168.0.126	192.168.0.127
192.168.0.128	255.255.255.240	14	192.168.0.129 to 192.168.0.142	192.168.0.143
192.168.0.144	255.255.255.240	14	192.168.0.145 to 192.168.0.158	192.168.0.159
192.168.0.160	255.255.255.240	14	192.168.0.161 to 192.168.0.174	192.168.0.175
192.168.0.176	255.255.255.240	14	192.168.0.177 to 192.168.0.190	192.168.0.191
192.168.0.192	255.255.255.240	14	192.168.0.193 to 192.168.0.206	192.168.0.207
192.168.0.208	255.255.255.240	14	192.168.0.209 to 192.168.0.222	192.168.0.223
192.168.0.224	255.255.255.240	14	192.168.0.225 to 192.168.0.238	192.168.0.239
192.168.0.240	255.255.255.240	14	192.168.0.241 to 192.168.0.254	192.168.0.255

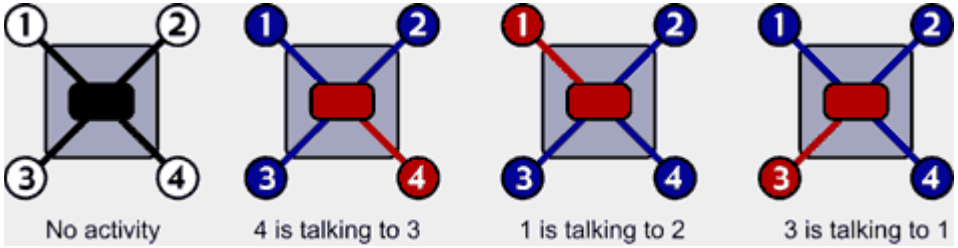
HUBS vs SWITCHES

In order to network computers together, they need to be somehow physically connected to each other. While it is possible to daisy-chain multiple computers together (i.e., in one port, out another) into a network, it is more efficient to tie all of them into a single device.
Hubs and switches serve that purpose, and from the outside, they function identically: allowing connected computers to exchange data among themselves. However, the way they handle data internally is very different.

HUBS - Half-duplex 'dumb' network device

allow all devices that are connected to them to communicate to each other.
A hub makes no decisions about traffic direction, it doesn't inspect traffic quality or verify packet integrity.
All network data received on one port will be immediately transmitted out all the other ports, so each computer must take it's turn before sending data.
Analogous to telephone party line.





Hop count rules limit the number of hubs that can be interconnected between two computers

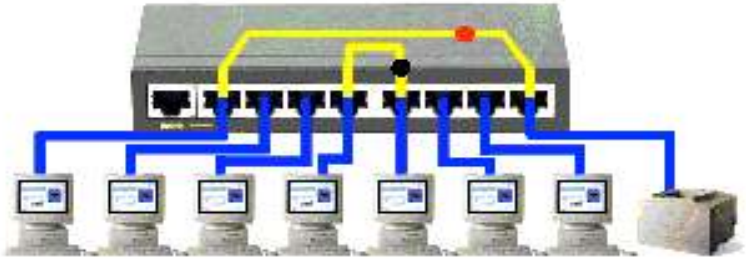
SWITCHES - full duplex 'smart' hub

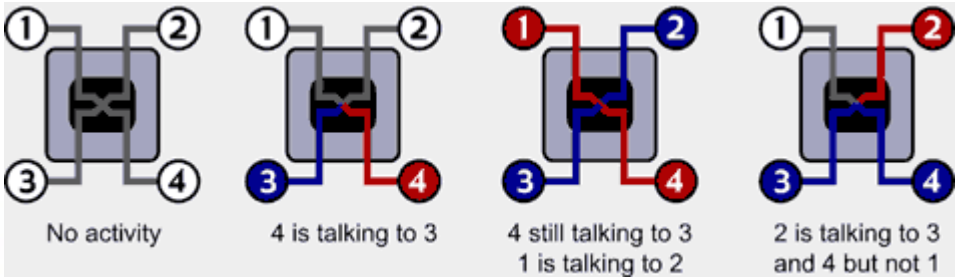
Actively looks at the traffic it receives and based on the destination address it will direct that traffic only to the port needed. The switch listens to each port at the same time without any interference.

A computer plugged directly into the switch will not receive unnecessary traffic and can transmit to the switch whenever it needs to.

Switch memorizes the MAC address of each host and which port it resides on. This is how it can intelligently direct traffic.

There are no limits to the number of switches that can be interconnected between two computers.





If you already have purchased several hubs and are experiencing a slow network, a single switch can solve your problem. Instead of having all hubs daisy chained together, you can separate them with the switch as the center point between all the hubs. This will avoid traffic propagating to the other hubs.

COTS 10/100 switches are cheap enough these days to justify their use rather than hubs in our network implementations

GATEWAYS

A network gateway is an internetworking system that joins two networks together. A network gateway can be implemented completely in software, completely in hardware, or as a combination of the two.
Because a network gateway by definition appears at the edge of a network, related functionality like firewalling tends to be installed on the network gateway.

ROUTERS

A router is a networking device that forwards data packets to their destinations. Routing occurs at layer 3 of the OSI model. A router can be used to either connect at least two networks, or to form a mobile ad-hoc network.

An Edge router connects end-users to the Internet; a Core router transmits data between other routers.A router creates and/or maintains a "routing table" that stores the best routes to network destinations and the "routing metrics" associated with those routes.

Routers are now being implemented as Internet gateways, primarily for small networks (SOHO). This application is mainly where the Internet connection is an always-on broadband connection like cable modem or DSL.
These are not "routers" in the true sense, but the terminology has been confused with network address translation.

SOHO router Gateway mode should be used if your device hosts your network's connection to the Internet. Router mode should be selected if the router exists on a network with other routers, including a separate network gateway.

WIRELESS ROUTERS

A network router that provides wireless connectivity. It is not uncommon to find combination COTS devices from various vendors which include any/all of the following features: cable modem / router / switch and wireless connectivity. Such devices are relatively cheap and accessible for rapid deployment.

DHCP Dynamic Host Configuration Protocol

Assigns dynamic IP addresses to devices on a network. With dynamic addressing, a device can have a different IP address every time it connects to the network. In some systems, the device's IP address can even change while it is still connected. DHCP also supports a mix of static and dynamic IP addresses.

Dynamic addressing simplifies network administration because the software keeps track of IP addresses rather than requiring an administrator to manage the task. This means that a new computer can be added to a network without having to manually assigning a unique IP address.

NAT Network Address Translation

Enables a local-area network (LAN) to use one set of non routable IP addresses for internal traffic and a second set of addresses for external traffic. A NAT device located at the LAN/Internet junction makes all IP address translations.

NAT serves three main purposes:

- Provides a type of firewall by hiding internal IP addresses
- Enables use of more internal IP addresses with no conflict with routable IPs
- Allows user to combine multiple ISDN connections into a single Internet connection

WIRELESS ACCESS POINTS

A wireless access point (AP) connects wireless communication devices together to create a wireless network. The AP is usually connected to a wired network, and can relay data between devices on each side. Many APs can be connected together to create a larger network that allows "roaming".

One IEEE 802.11 WAP can typically communicate with 30 client systems within a radius of 100 m. However, communication range can vary a lot depending on such variables as indoor or outdoor placement, height above ground, nearby obstructions, type of antenna, the current weather, operating radio frequency, and power output of the device.

WIRELESS REPEATERS

Provide a way to extend the range of an existing WLAN instead of adding more access points. There are very few stand-alone 802.11 wireless repeaters on the market, but some access points have a built-in repeater mode.

In general, a repeater simply regenerates a network signal in order to extend the range of the existing network infrastructure. A repeater does not physically connect by wire to any part of the network. Instead, it receives radio signals (802.11 frames) from an access point, end user device, or another repeater and retransmits the frames. This makes it possible for a repeater located in between an access point and distant user to act as a relay for frames travelling back and forth between the user and the access point.

WIRELESS BRIDGES

A wireless LAN bridge can interface an Ethernet network directly to a particular access point. A bridge plugs into the Ethernet network and uses the 802.11 protocol to communicate with an AP within range. thus wirelessly connecting a cluster of users (actually a network) to an AP.
Wireless bridges are a very practical, easy, and in most cases inexpensive way to connect Ethernet LANs or extend the range of existing WLANs. They are quick to set up and easy to configure, making them an ideal choice to quickly set up voice and data networks.

Types of WLAN Bridges

- Basic Ethernet-to-Wireless.

This type connects directly to a single device via an Ethernet port, and then provides a wireless connection to an access point. These types of connections offer a substitute for a radio NIC; making it useful when the device, such as a printer, PC, or video game console, has an Ethernet port and no 802.11 NIC.

- Workgroup Bridges.

Connect wireless networks to larger, wired Ethernet networks. Essentially a workgroup bridge acts as a wireless client on the wireless LAN and then interfaces to a wired network. The wired side may connect directly with a single device (like an Ethernet-to-Wireless bridge) or to an Ethernet hub or switch that connects multiple devices.

- Access Point / Wireless Bridge Combos.

Some vendors offer access points that you can configure as a bridge, but not both at the same time.

POWERLINE / HOMEPLUG BRIDGES

Electrical power is supplied and distributed around the house at 60Hz.
Electrical wiring is capable of carrying a range of other frequencies which can be 'tuned-in' using appropriate equipment. Powerline technology takes advantage of this unused bandwidth of the electrical wiring in the home.

PowerLine devices plug into the electrical socket and draws power for the device.
At the same time, it sends data signals across the house wiring.
A second PowerLine device can then be placed on any electrical outlet in the home/office to receive the signal.

Range on Powerline can be expected to be 100m or more.
Generally any circuit working on the same electricity meter will provide a good connection. Will not work through surge protectors / signal conditioning hardware

Be aware of country power differences:
50Hz 220V / 60Hz 110V

14 Mbps

HOMEPLUG Powerline Alliance
www.homeplug.org

LOOK FOR THIS LOGO

POWER OVER ETHERNET

"Active Ethernet" eliminates the need to run 110/220 VAC power to Wireless Access Points and other devices on a wired LAN. Using Power-over-Ethernet system installers need to run only a single CAT5 Ethernet cable that carries both power and data to each device. This allows greater flexibility in the locating of AP's and network devices and significantly decreasing installation costs

Power-over-Ethernet begins with a CAT5 "Injector" that inserts a DC Voltage onto the CAT5 cable. Some Wireless Access Points and other network accept the injected DC power directly from the CAT5 cable through their RJ45 jack. These devices are considered to be "PoE-Compatible" or "Active Ethernet Compatible".

Devices that are not "PoE Compatible" can be converted to POE by way of a DC "Picker" or "Tap". These are sometimes called Active Ethernet "Splitters". This device picks-off the DC Voltage injected into the CAT5 cable by the Injector and makes it available to the equipment through the regular DC power jack.

IEEE 802.3af

www.PowerOverEthernet.com

Power Over Ethernet

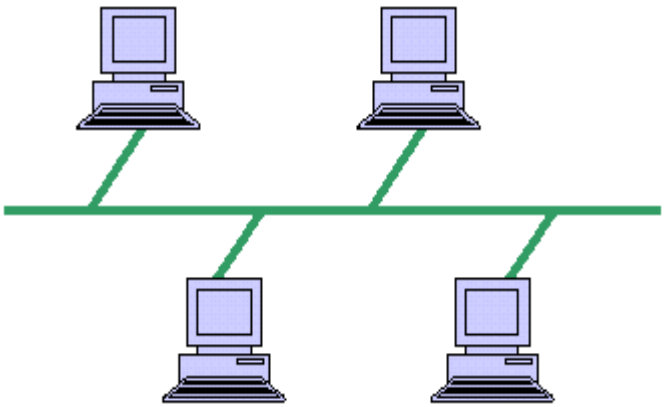
NETWORK TOPOLOGIES

Categorized into the following basic types: BUS, RING, STAR, TREE, MESH

More complex networks can be built as hybrids of two or more of these.

BUS

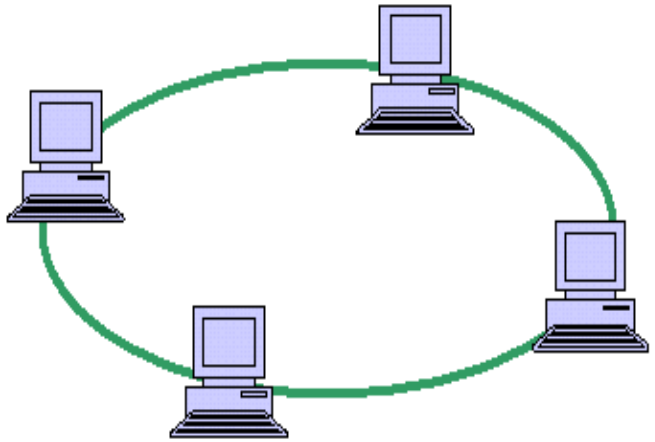
Bus networks use a common backbone to connect all devices. A single cable, the backbone functions as a shared communication medium, that devices attach or tap into with an interface connector.
A device wanting to communicate with another device on the network sends a broadcast message onto the wire that all other devices see, but only the intended recipient actually accepts and processes the message.



RING

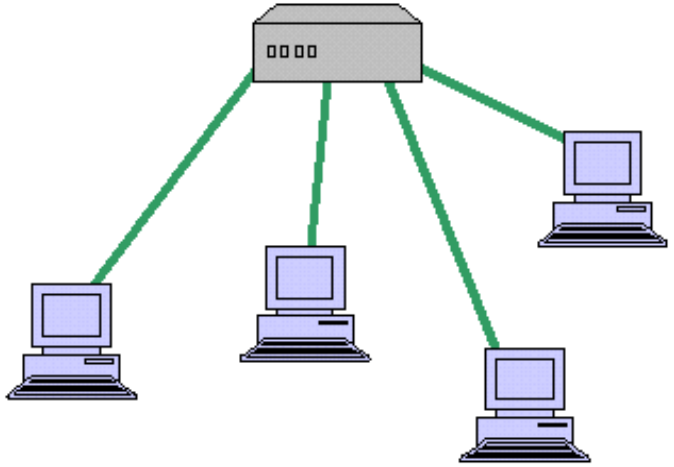
In a ring network, every device has exactly two neighbors for communication purposes. All messages travel through a ring in the same direction
A failure in any cable or device breaks the loop and can take down the entire network.

To implement a ring network, one typically uses FDDI, SONET, or Token Ring technology. Rings are found in some office buildings or school campuses.



STAR

Many home networks use the star topology.
A star network features a central connection point called a "hub" that may be an actual hub or a switch. Devices typically connect to the hub with Unshielded Twisted Pair (UTP) Ethernet.



A star network generally requires more cable, but a failure in any star network cable will only take down one computer's network access and not the entire LAN.

TREE

Tree topologies integrate multiple star topologies together onto a bus. In its simplest form, only hub devices connect directly to the tree bus, and each hub functions as the "root" of a tree of devices. This bus/star hybrid approach supports future expandability of the network much better than a bus (limited in the number of devices due to the broadcast traffic it generates) or a star (limited by the number of hub ports) alone.

MESH

Mesh topologies involve the concept of routes. Unlike each of the previous topologies, messages sent on a mesh network can take any of several possible paths from source to destination. (Recall that in a ring, although two cable paths exist, messages can only travel in one direction.)
Some WANs, like the Internet, employ mesh routing.

PRODUCT SHOWCASE

Sample of hardware in possession and used for field deployments.
Presented for reference purposes only.
Router / AP Brands are only representative of current stage of field test success.

KEY POINTS TO REMEMBER:

BRAND AGNOSTIC

RTFM

WEAR A SAFETY PIN

KNOW DEFAULT ADMIN PASSWORDS

STICKY LABEL with CURRENT IP SETTINGS

CANTENNA

12dBi 30° directional antenna

Pros:

12 dBi gain
Directional
Narrow Beam
Cheap / Disposable
Easy connection to AP, bridges, etc
Local San Diego company

Cons:

Need wifi card with external connector for use with laptop

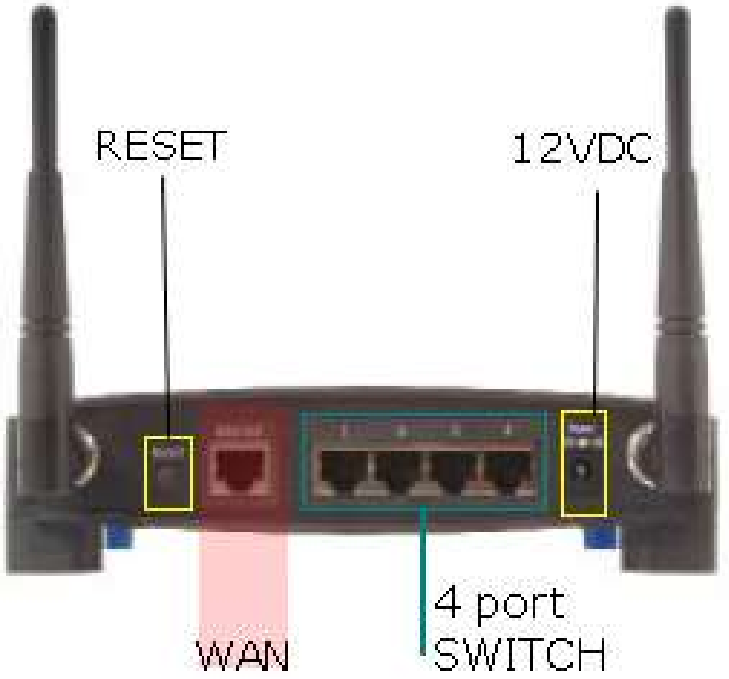
www.cantenna.com

LINKSYS WRT54G

Internet sharing Router,
4-port Switch and 802.11g AP

Operating features:
DHCP ,NAT, MAC Filters
DMZ , Port forwarding, Routing
DDNS, Web interface

Defaults
IP: **192.168.1.1** netmask FFFFFF00
UserName: *<blank>*
Password : admin
Reset switch: depress 10 sec : RESTORE
: momentary : REBOOT



PROS:

- ☑ Firmware flashable to linux version allowing for higher power settings and more advanced control. (Sveasoft.com)
- ☑ 12 VDC powered
- ☑ Removable antennas

CONS:

- ☒ Bulky form factor
- ☒ Bulky default power supply

LINKSYS WAP54G

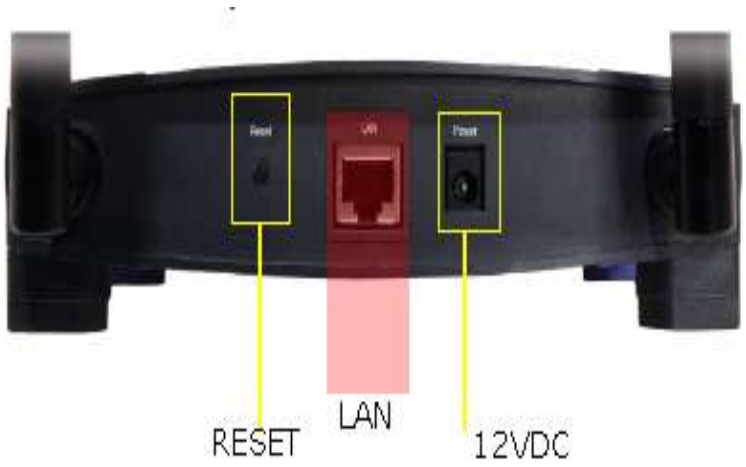
802.11g AP

Operating features:
AP / Wireless Bridge modes
MAC Address filter, SNMP
Web interface

Defaults
IP: **192.168.1.245** netmask FFFFFF00
UserName: *<blank>*
Password : admin
Reset switch: depress 10 sec : RESTORE

PROS:

- ☑ Firmware flashable to linux version allowing for higher power settings and more advanced control (Sveasoft.com)
- ☑ 12 VDC powered
- ☑ Removable antennas



CONS:

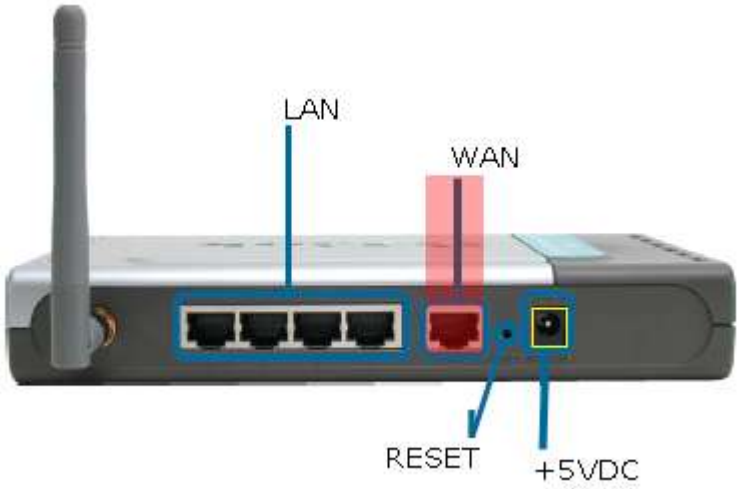
- ☒ Bulky form factor
- ☒ Bulky default power supply
- ☒ Wireless bridge exclusive (per manual) mode requires other linksys wireless bridge

DLINK DI-614+ revB

Internet Sharing Router
4 port switch, 802.11b AP

Operating features:
DHCP, Port forwarding, IP/MAC filters,
URL/Domain blocking, firewall, DMZ, DDNS
Variable transmit power (10 – 17 dBm)
Web interface

Defaults
IP: **192.168.0.1** netmask FFFFFF00
UserName: admin
Password : *<blank>*
Reset switch: depress 10 sec : RESTORE



PROS:

- ☑ Small form factor
- ☑ Small default power supply
- ☑ Removable antenna

CONS:

- ☒ 5VDC, 2A power supply

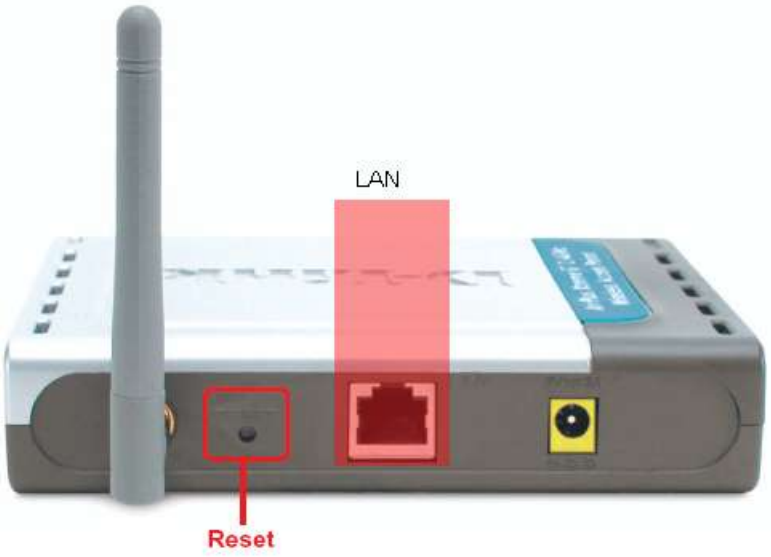
Web emulator: http://support.dlink.com/emulators/di614+_revB/

DLINK DWL-2100AP

802.11g multimode AP

Operating features:
AP / PtP Bridge / PtMP Bridge
AP Repeater / AP Client
Variable transmit power
MAC Address filter, DHCP, SNMP
Web interface

Defaults
IP: **192.168.0.50** netmask FFFFFF00
UserName: admin
Password : *<blank>*
Reset switch: depress 6 sec : RESTORE



PROS:

- ☑ Small form factor
- ☑ Small default power supply
- ☑ Removable antenna

CONS:

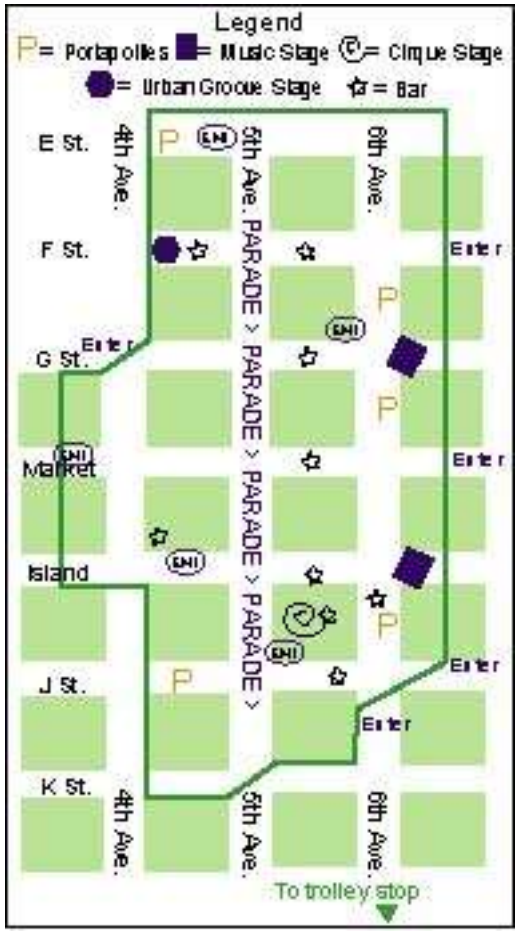
- ☒ 5VDC, 2A power supply
- ☒ Bridge mode dlink exclusive

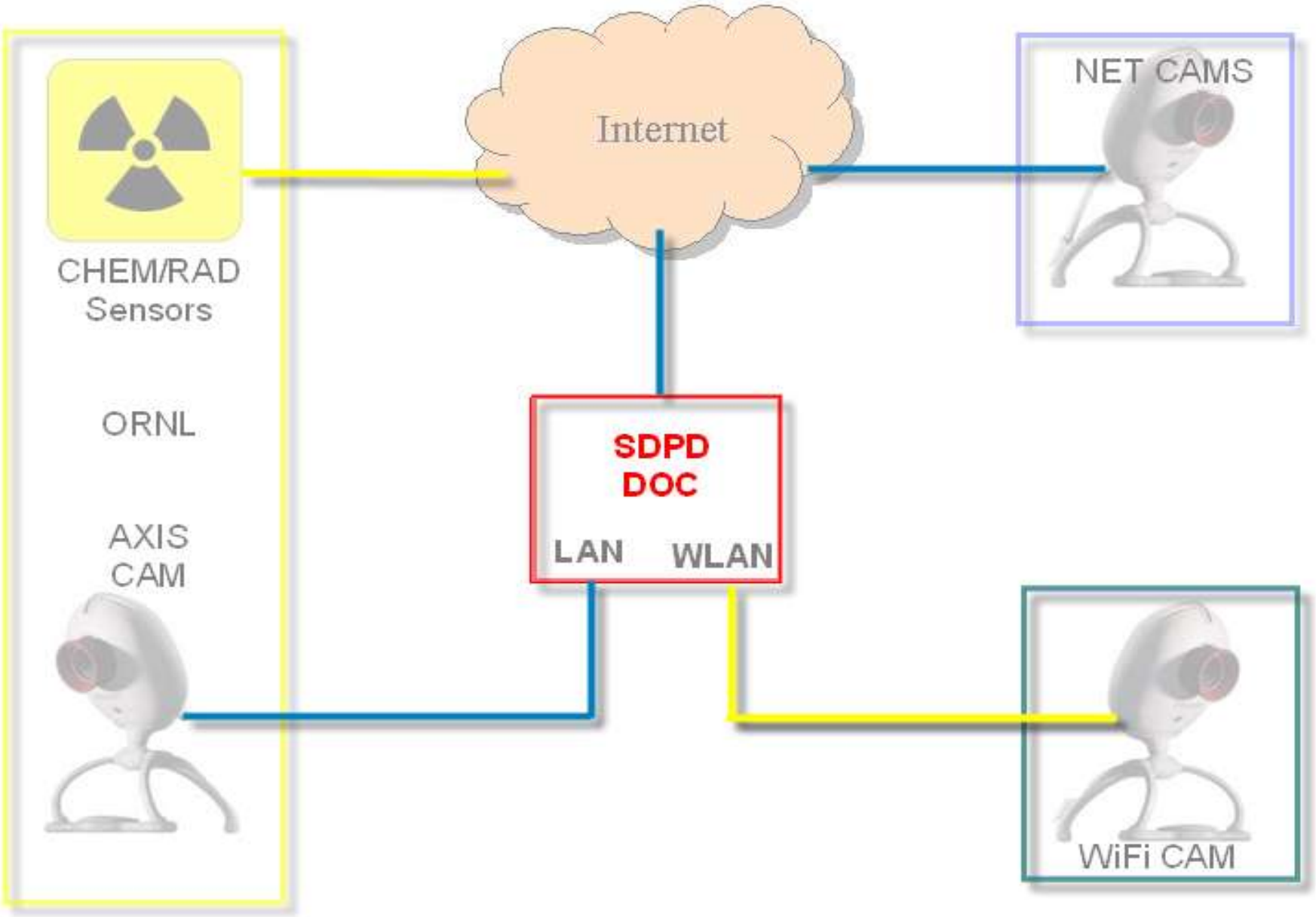
Web emulator: http://support.dlink.com/techtool/dwl2100ap/emulator/

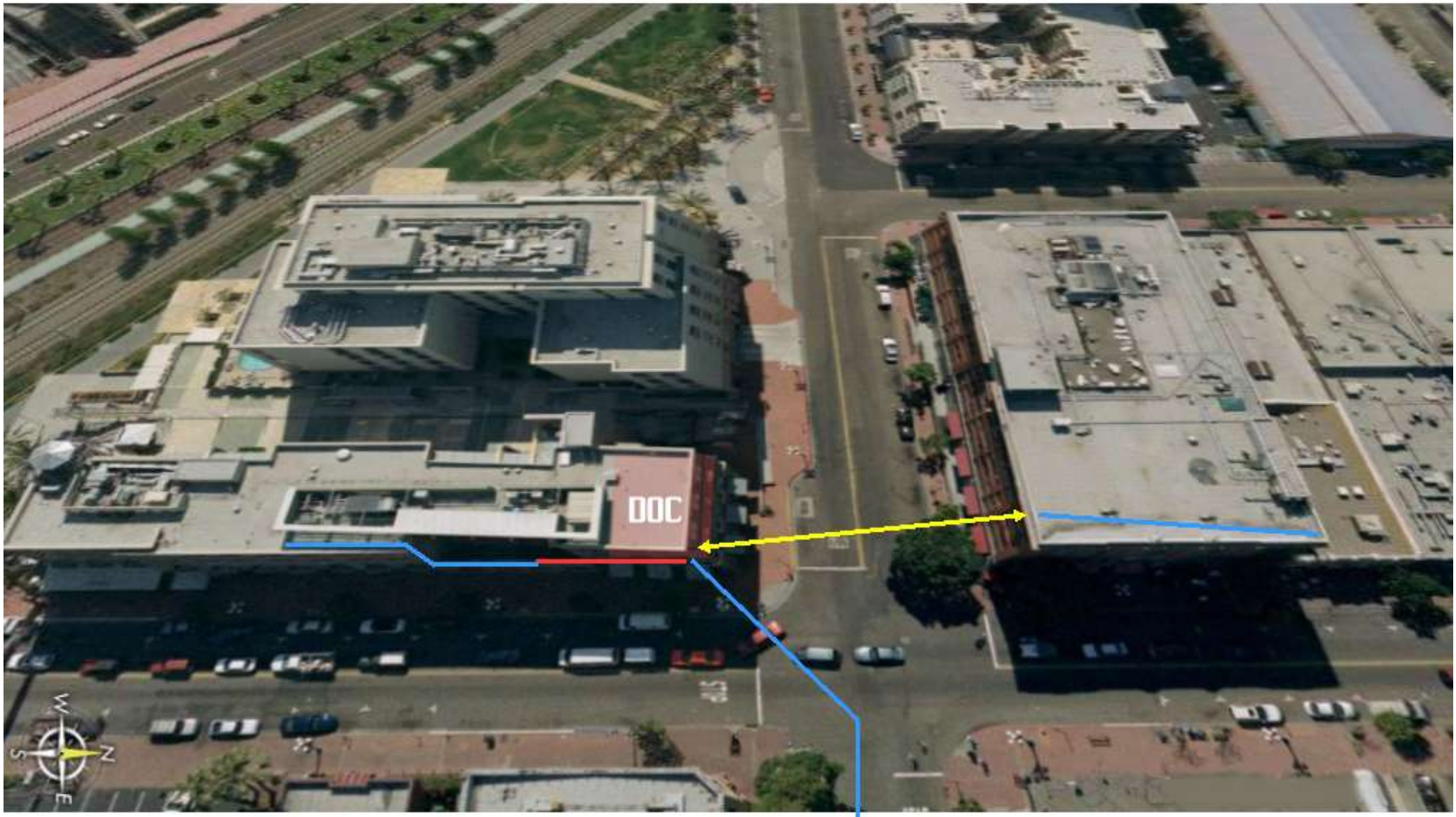
EXAMPLE NETWORK IMPLEMENTATION

Location: San Diego Mardi Gras, Feb 08 2005

Purpose: Provide network support for SDPD and ORNL
Deploy internet based sensor cameras
Leverage existing city camera infrastructure




Internet
NET CAMS
CHEM/RAD
Sensors
ORNL
AXIS
CAM
SDPD
DOC
LAN
WLAN
WiFi CAM

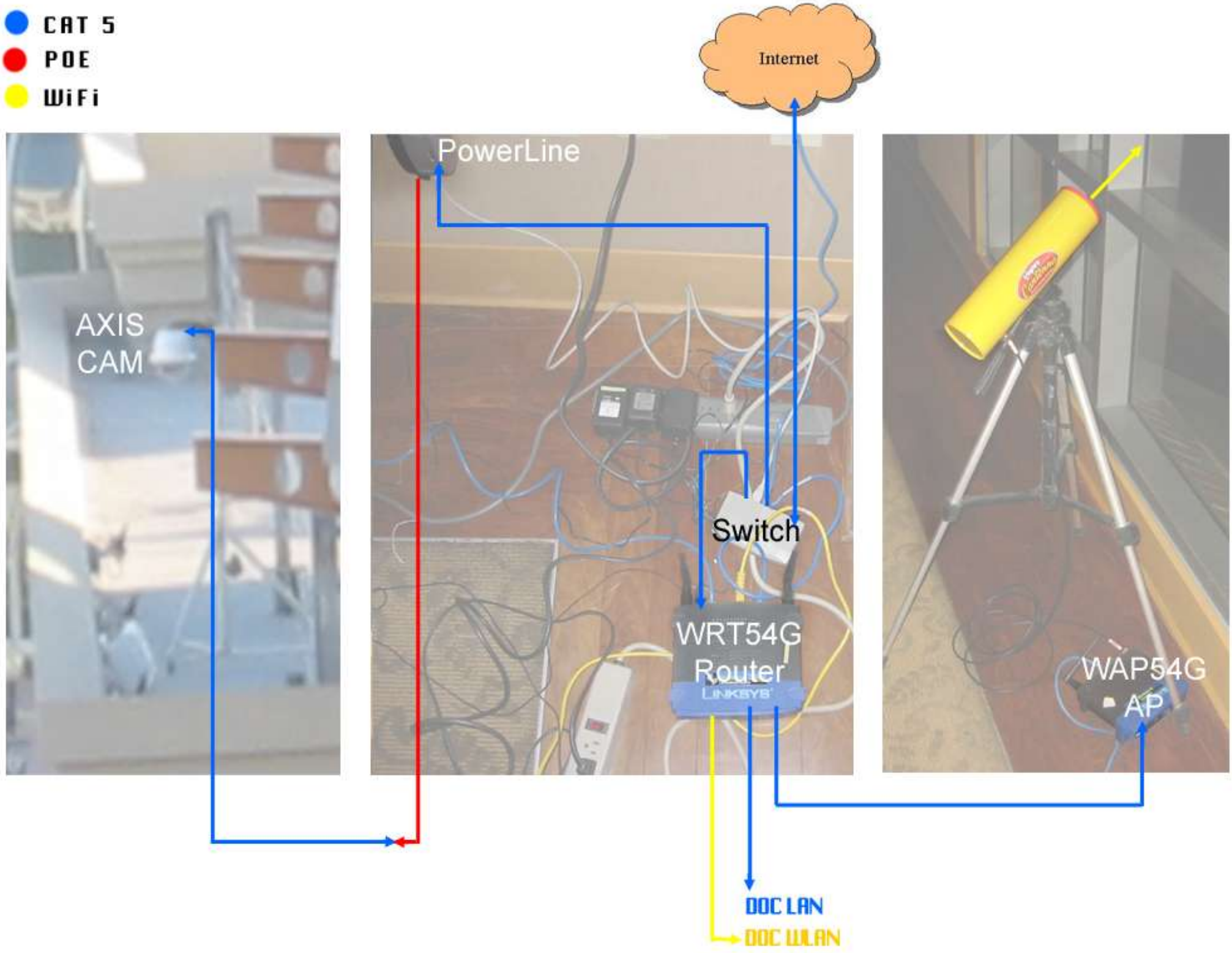


POE

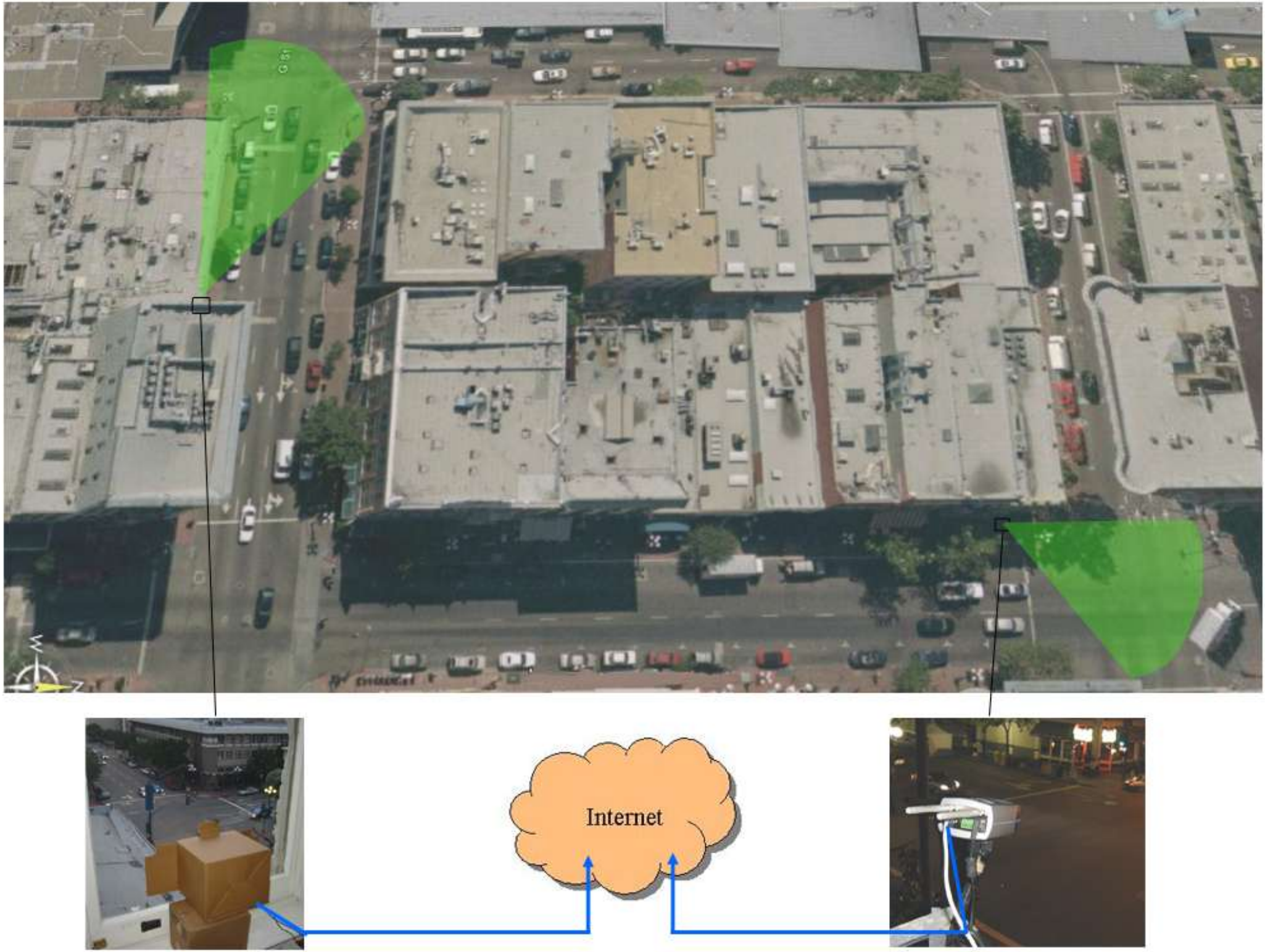
WiFi

CAT 5

Internet


CAT 5
POE
WiFi
Internet
PowerLine
AXIS
CAM
Switch
WRT54G
Router
LINKSYS
WAP54G
AP
DOC LAN
DOC WLAN

DWL 2100AP
in AP CLIENT mode


Internet