Network Architecture and Security

Contents

What is the Internet?

The Internet is formed by billions of connected computing devices, communication links and packet switches:

- It is the network of networks: interconnected ISPs (Internet Service Providers)
- Protocols define format and control sending, receiving of messages
    - E.g. TCP, IP, HTTP, Skype, 802.11
- Standards
    - RFC (Request for comments), IETF (Internet Engineering Task Force)
- Provides services to applications (Web, VoIP, email, social nets, …)
- Provides programming interface to apps

Internet structure

The Internet can be described according to the following structure:

1. Network edge: formed by hosts and servers
2. Access networks: wired and wireless communication links provide access to the Internet
3. Network core: a mesh of interconnected routers which switch packets and interconnect access networks and network edge

Internet uses Packet-switching to send data:

- Hosts break application-layer messages into packets
- Forward packets from one router to the next, across links on path from source to destination

At center (network core): small number of well-connected large networks

- “tier-1” commercial ISPs (e.g., Level 3, Sprint, AT&T, NTT), national & international coverage
- Content provider network (e.g., Google): private network that connects its data centers to Internet, often bypassing tier-1, regional ISPs
- Internet Exchange Points (IXP) which interconnect Tiers
- Points of Presence (PoP) where Tiers’ clients interconnect

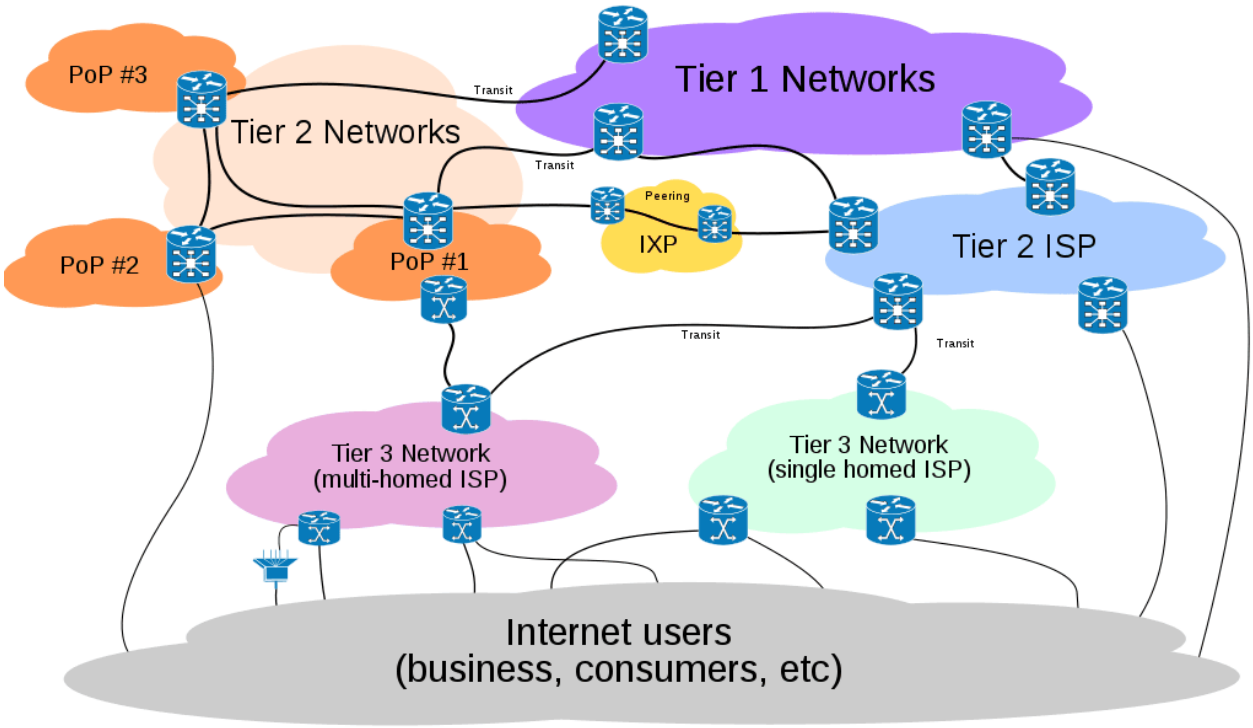


Figure 1 Structure of the Internet Core Network
View on tier 1 and 2 ISP interconnections by Ludovic.ferre from Wikipedia CC BY-SA 3.0

Users connect to Internet through access networks: Public Switched Telephone network, Cable Operator, ADSL …

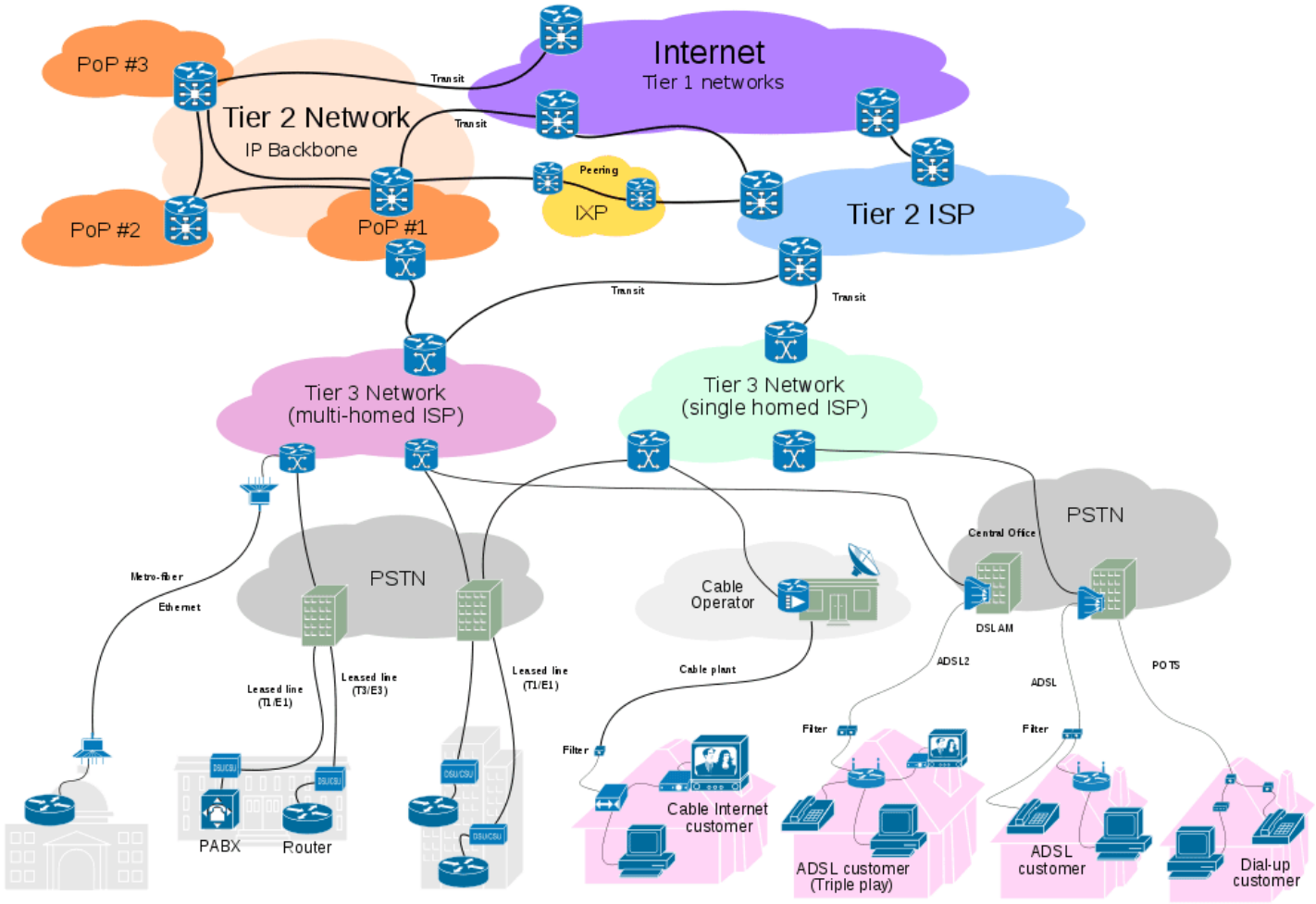


Figure 2 Different Access Networks connect to Internet Service Providers
Diagram showing how customers connect to ISP's... by Ludovic.ferre from Wikipedia CC BY-SA 3.0

Network Architecture and Security

Protocol layers

Networks are complex, with many "pieces": Hosts, routers, links of various media, applications, protocols, hardware, software, …

How to deal with complex systems? The answer is "Layering" …

- Layering explicit structure allows identification, relationship of complex system's pieces
- Modularization eases maintenance, updating of system
    - Change of implementation of layer's service transparent to rest of system
    - e.g., change in gate procedure doesn't affect rest of system

Internet protocol stack

The Internet protocol stack is defined in terms of four or five layers. Link and physical layers sometimes are joined and presented together. The five layers are:

- *Application*: supporting network applications
    - FTP, SMTP, HTTP, Twitter, Facebook, …
- *Transport*: process-process data transfer
    - TCP, UDP
- *Network*: routing of datagrams from source to destination
    - IP, routing protocols
- *Link*: data transfer between neighboring network elements
    - Ethernet, 802.11 (WiFi), PPP, Bluetooth, …
- *Physical*: bits "on the wire"

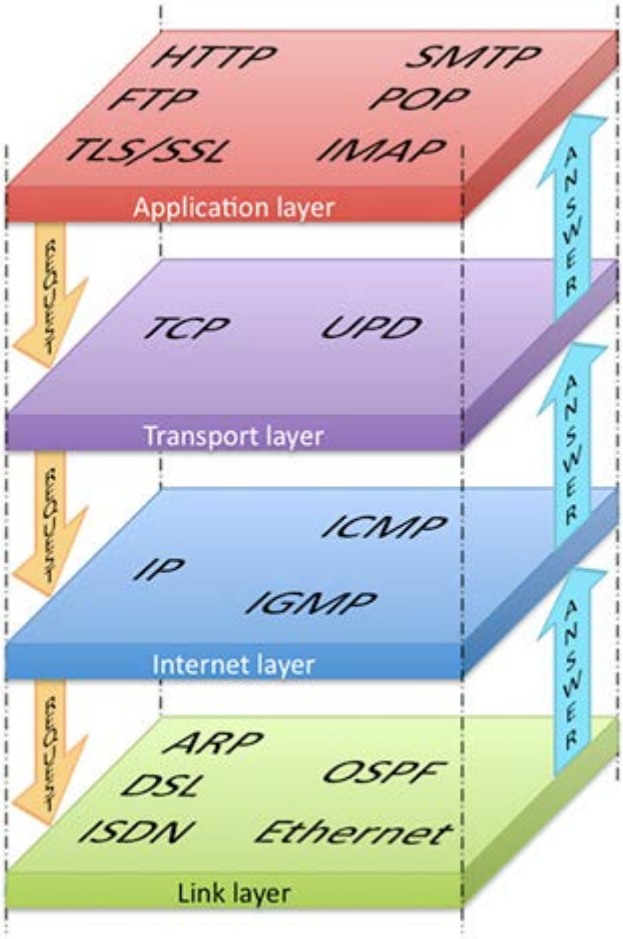


Figure 3 Internet Protocol Stack
A graphic representation of the Internet Protocol Stack...
by Bughunter (Own work) from Wikipedia Public Domain

The network layer

The main function of the Network Layer is to transport segments from sending to receiving host:

- On sending side encapsulates segments into datagrams
- On receiving side, delivers segments to transport layer
- Network layer protocols are in every host and router
- Router examines header fields in all IP datagrams passing through it

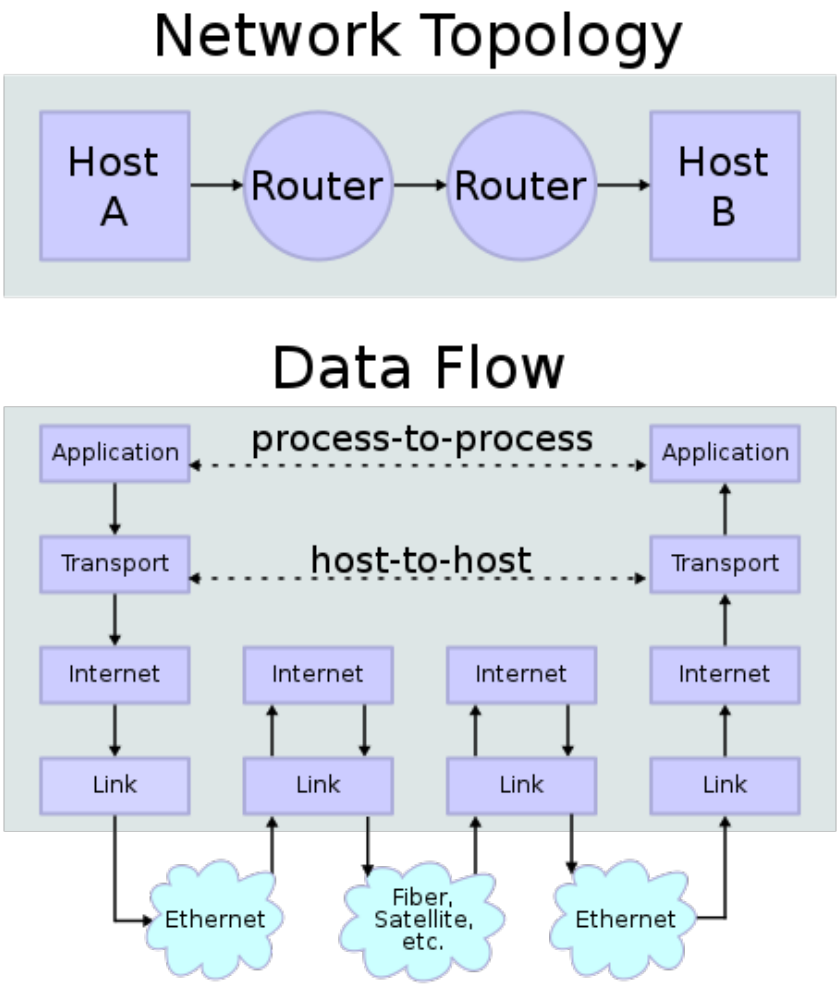


Figure 4 The Data Flow in the Internet Protocol Stack
Operation of the Internet Protocol suite between two Internet hosts connected via two routers ... by Kbrose from Wikipedia CC BY-SA 3.0

Network layer: data plane, control plane

The network layer consists of a data plane and a control plane:

- Data plane
  - Determines how datagram arriving on router input port is forwarded to Router output port
  - It has a forwarding function from a local perspective
- Control plane
  - Covers network-wide logic
  - Determines how datagram is routed among routers along end-end path from source host to destination host

- There are two control-plane approaches:
  - Traditional routing algorithms: implemented in routers
  - Software-defined networking (SDN): implemented in (remote) servers (in the next figure we have an example of an opensource SDN architecture)

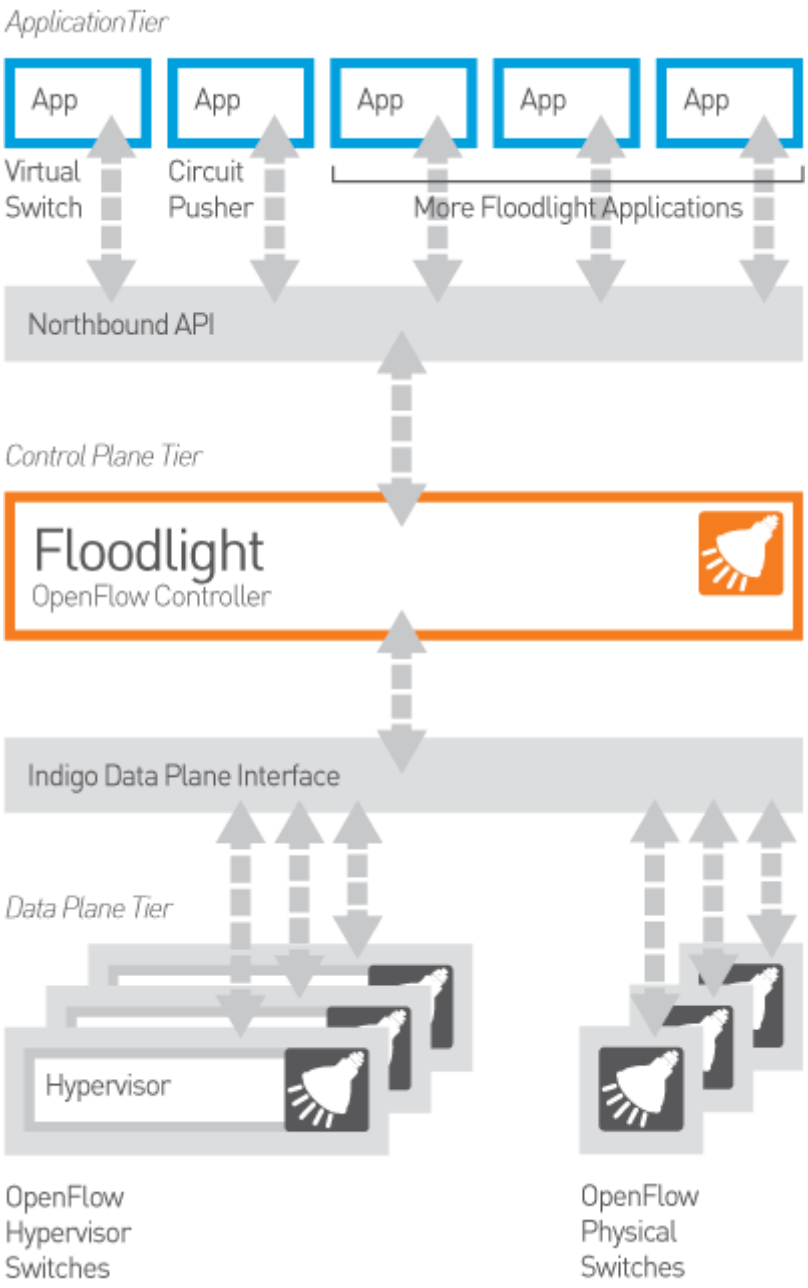


Figure 5 An example of Software Defined Network architecture
Meat Atlas - Meat demand in emerging national economies is on the rise by Heinrich Boell Foundation... from Wikipedia CC BY-SA

Destination-based forwarding

Forwarding is based on destination address ranges. However, it may happen that ranges do not divide so nicely. Then … apply Longest Prefix Matching. When looking for forwarding table entry for given destination address, use longest address prefix that matches destination address.

Destination Address Range	Link interface
11001000 00010111 00010* ********	0
11001000 00010111 00011000 ********	1
11001000 00010111 00011* ********	2
Otherwise	3

The table above shows four destination address ranges. The first three ranges share the first twenty bits. The twenty first bit is the same for the second and third entries. However, the second entry is followed by wildcards and the third one is followed by three bits and then wildcards. The fourth entry is otherwise, which means that if a destination address does not match any prefix, this is the selected entry. In the example, a destination address matches the second and third entries, but the coincidence extends three more bits in the third entry. Thus, this is the final selection.

Question

Which interface will be selected in the router?

DA: 11001000 00010111 00010110 10100001

DA: 11001000 00010111 00011000 10101010

Answer

1. Interface 0
2. Interface 1

Internet network layer

The main function of the network layer is to forward packets from an origin to a destination.

- The IP protocol implements addressing conventions, datagram format and packet handling conventions
- The routing protocols configure the routers' forwarding tables to perform efficient path selection
    - RIP, OSPF and BGP are the facto routing protocols in the Internet

The IPv4 (IP version 4) datagram has the following format:

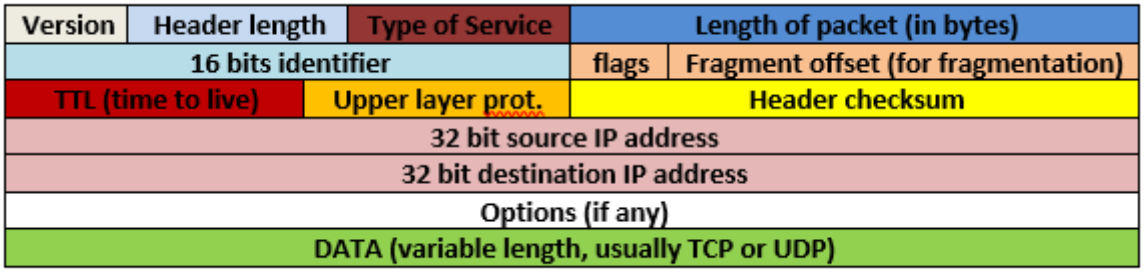


Figure 7 IPv4 Datagram format

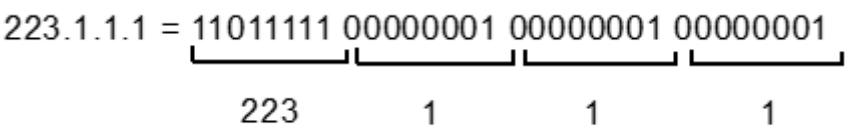
Usually, an IP packet has a 20 bytes header without options. Header Length is the number of 32 bits header words. Type of Service can be used to define the "type" of data. Every IP packet has a 16 bits identifier. Flags and Fragment offset are used in IP fragmentation. Fragmentation occurs when IP packets are bigger than the Maximum Transfer Unit (MTU) of a link. TTL determines the maximum number of hops permitted to the packet. The Upper layer protocol specifies the protocol used in the DATA field. Next we have the header checksum and the 32 bits source and destination addresses.

IP addressing

An IP address is a 32-bit identifier for host and router interfaces

- The interface is a connection between host/router and physical link
    - Routers typically have multiple interfaces
    - Host typically has one or two interfaces (e.g., wired Ethernet, wireless 802.11)

- IP addresses are associated with each interface
- An IP address is represented as a sequence of four bytes in decimal. Each byte is separated by a dot.



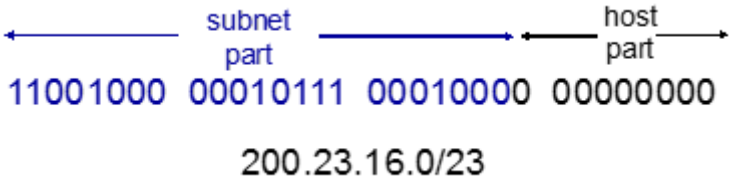
IP address

IP addressing: CIDR

CIDR stands for Classless Interdomain Routing

- Each IP address has a portion of arbitrary length which defines a subnet

The address format is a.b.c.d/x, where x is the number of bits in subnet portion of address



Classless Interdomain Routing

- A subnet is formed by device interfaces with same subnet part of IP address
    - Can physically reach each other without intervening router

Question

How many subnets can you find?

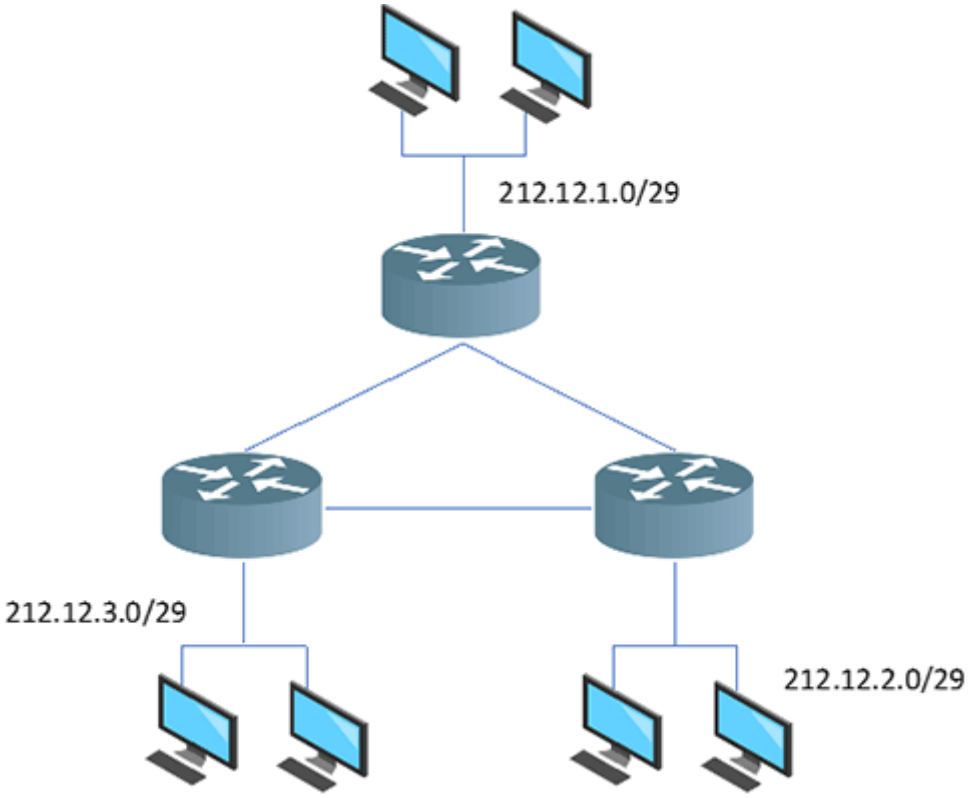


Figure 8 Network topology with three routers, three subnetworks and three links

Answer

6 subnets. We must consider also the three links which interconnect the routers.

IP addressing: how to get one?

- Hard-coded by system admin in a file
- DHCP: Dynamic Host Configuration Protocol
    - Dynamically get address from a server (plug-and-play)
    - Allows host to dynamically obtain its IP address from network server
    - Allows reuse of addresses
    - Support for mobile users who want to join network

DHCP: Dynamic Host Configuration Protocol

DHCP messages are encapsulated in UDP datagrams.

DHCP overview:

- Host broadcasts “DHCP discover” msg [optional]
- DHCP server responds with “DHCP offer” msg [optional]
- Host requests IP address: “DHCP request” msg
- DHCP server sends address: “DHCP ack” msg

DHCP can return more than just allocated IP address:

- Address of first-hop router
- Name and IP address of DNS server
- Network mask

Hierarchical addressing: route aggregation

It allows efficient advertisement or routing information.

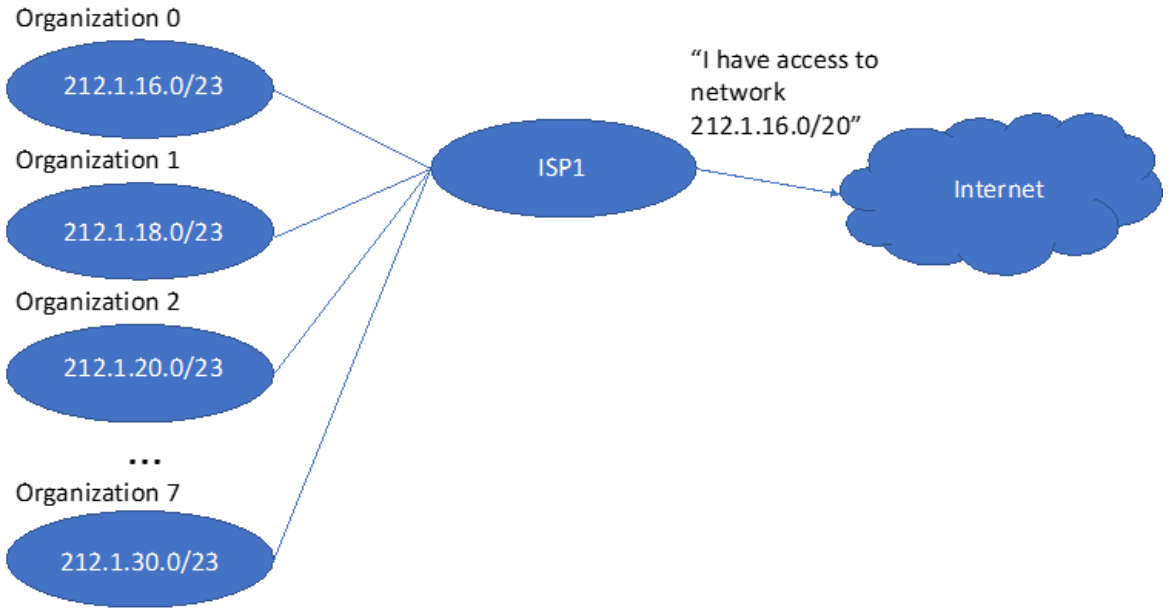


Figure 9 Several address ranges are aggregated by the ISP to simplify the advertisement of networks and configuration of routing tables

Question

Can you aggregate the following addresses?

1. 192.168.1.0/26
2. 192.168.1.64/26
3. 192.168.1.128/26
4. 192.168.1.192/26

Answer

192.168.1.0/24

NAT: Network Address Translation

Motivation: local network uses just one IP address as far as outside world is concerned:

- Range of addresses not needed from ISP: just one IP address for all devices
- Can change addresses of devices in local network without notifying outside world
- Can change ISP without changing addresses of devices in local network
- Devices inside local net not explicitly addressable, visible by outside world (a security plus)

NAT implementation

- Outgoing datagrams: replace (source IP address, port number) of every outgoing datagram to (NAT IP address, new port number)

  . . . remote clients/servers will respond using (NAT IP address, new port number) as destination address
- Remember in NAT translation table every (source IP address, port number) to (NAT IP address, new port number) translation pair
- Incoming datagrams: replace (NAT IP address, new port number) in destination fields of every incoming datagram with corresponding (source IP address, port number) stored in NAT table

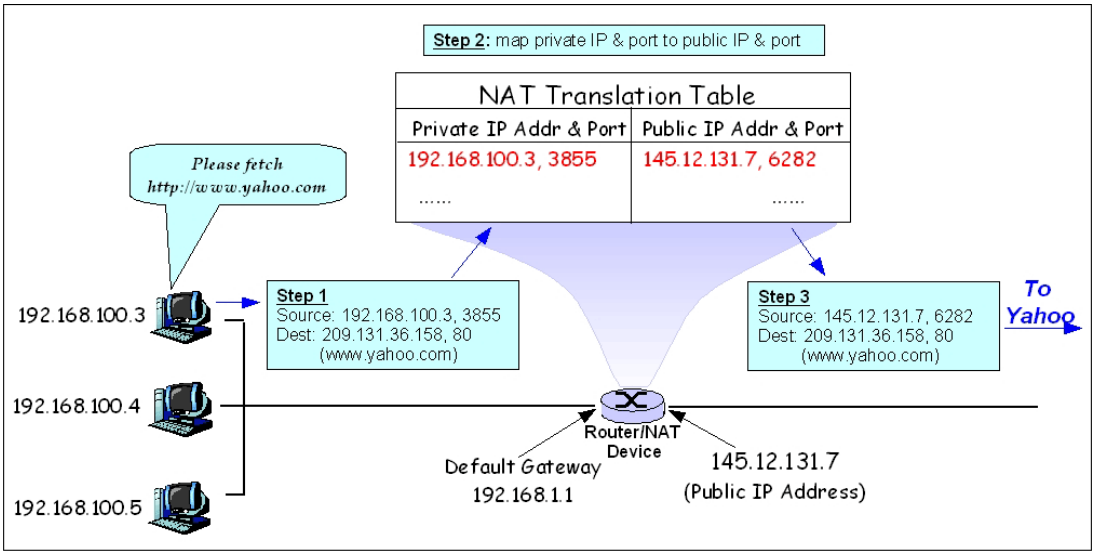


Figure 10 NAT router translates from private IP to public IP to send a datagram to the Internet en:/Images by Yangliy from Wikipedia Public Domain

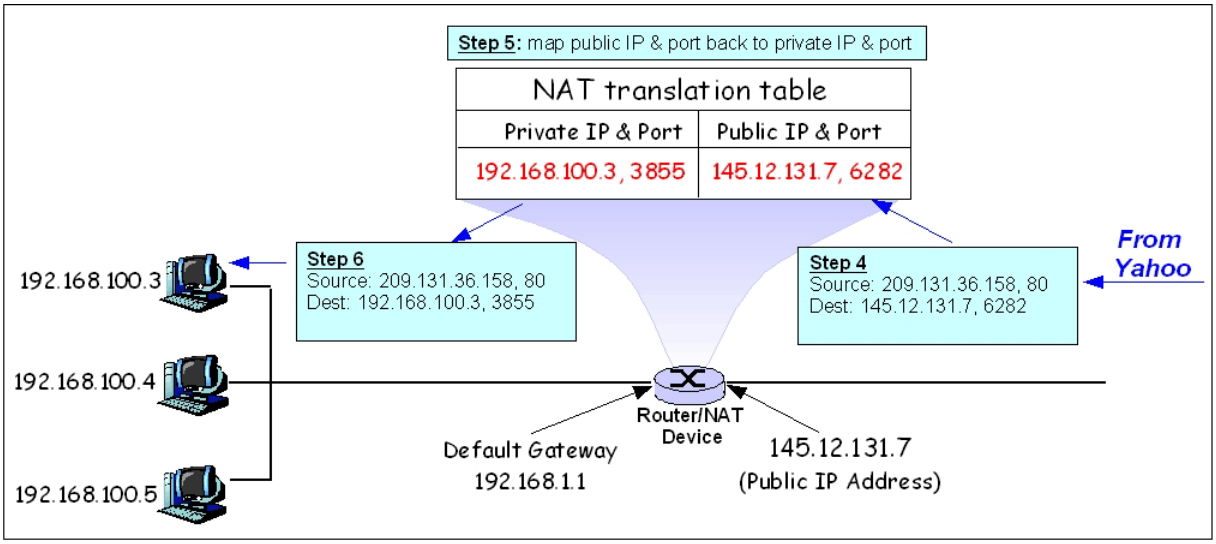


Figure 11 NAT router translates public IP to private IP to send a datagram from the Internet to the private network

self-created image of NAT for returning packet en:/Images by Yangliy from Wikipedia Public Domain

Routing protocols

Routing protocol goal is to determine "good" paths (equivalently, routes), from sending hosts to receiving host, through network of routers:

- Path: sequence of routers packets will traverse in going from given initial source host to given final destination host
- "good": least "cost", "fastest", "least congested"

Routing algorithms use graph abstractions of the network.

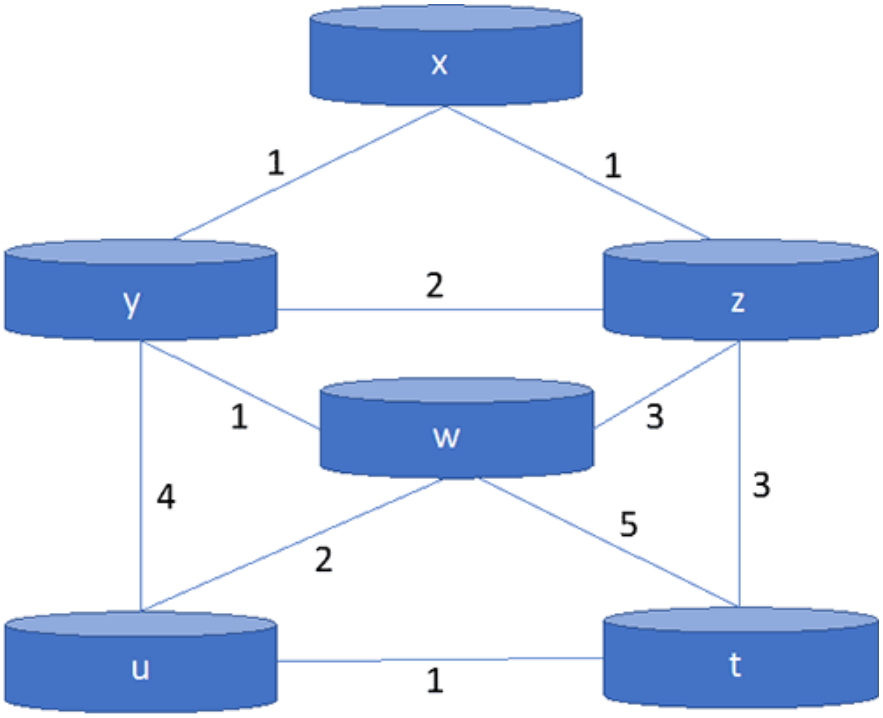


Figure 12 A graph abstraction of a network

Link-state routing algorithm

Dijkstra's algorithm:

- Needs the net topology and link costs known to all nodes
  - Accomplished via "link state broadcast"
  - All nodes have same info
- Computes least cost paths from one node ('source") to all other nodes
  - Gives forwarding table for that node
- It is iterative: after k iterations, know least cost path to k destination

Notation:

c(x,y): link cost from node x to y; = ∞ if not direct neighbours

D(v): current value of cost of path from source to dest. v

p(v): predecessor node along path from source to v

N': set of nodes whose least cost path definitively known

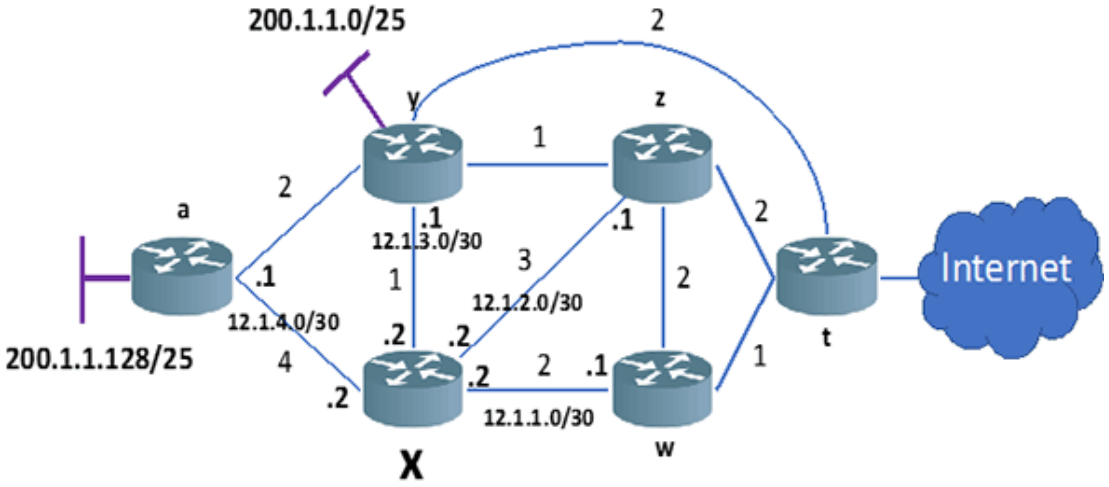


Figure 13 Example of IP network with link costs

The table below shows the resulting shortest-paths from X after the execution of the Dijsktra algorithm in router X:

Paso	N'	D(y), p(y)	D(z), p(z)	D(w), p(w)	D(a), p(a)	D(t),p(t)
0	x	1,x	3,x	2,x	4,x	inf
1	x,y	-	2,y	2,x	3,y	3,y
2	x,y,z	-	-	2,x	3,y	3,y
3	x,y,z,w	-	-	-	3,y	3,y
4	x,y,z,w,t	-	-	-	3,y	-
5	x,y,z,w,t,a	-	-	-	-	-

Figure 14 Computation of shortest paths using the Dijsktra algorithm

Once we have the shortest paths and the previous nodes to follow those paths, it is straightforward to obtain the spanning tree and then the forwarding table:

Spanning tree

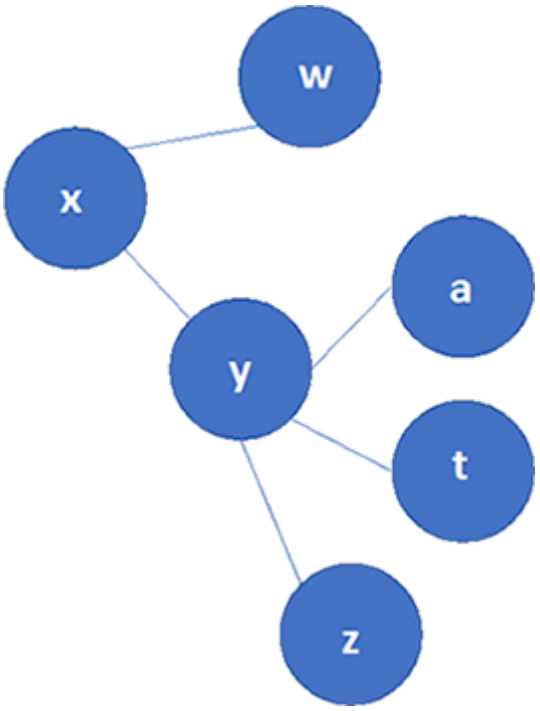


Figure 15 Spanning tree resulting from the execution of the Dijsktra algorithm in node X

Forwarding table

Destination	Next Hop
W	W
Y	Y
Z	Y
A	Y
T	Y

Routing table

Destination	Gateway (Next-hop)	Interface
Default	12.1.3.1	12.1.3.2

Figure 17 Resulting routing table in router X

Figure 17 shows a routing table. The first column represents the IP and network mask, i.e. the destination network. The second column shows the gateway or next-hop IP. This is the IP of the router where the packet must be sent to reach a destination. The last column is the interface which defines the outgoing port of the router where it must send the packet.

Internet approach to scalable routing

Aggregate routers into regions known as “autonomous systems” (AS). We distinguish between Intra-AS and Inter-AS routing.

Intra-AS routing protocols configure routers to make possible routing among host, routers in same AS (“network”). All routers in AS must run same intra-domain protocol. Routers in different AS can run different intra-domain routing protocol. A gateway router is at “edge” of its own AS, has link(s) to router(s) in other AS’es.

Inter-AS routing is focused on routing among AS’es. Gateways perform interdomain routing (as well as intra-domain routing).

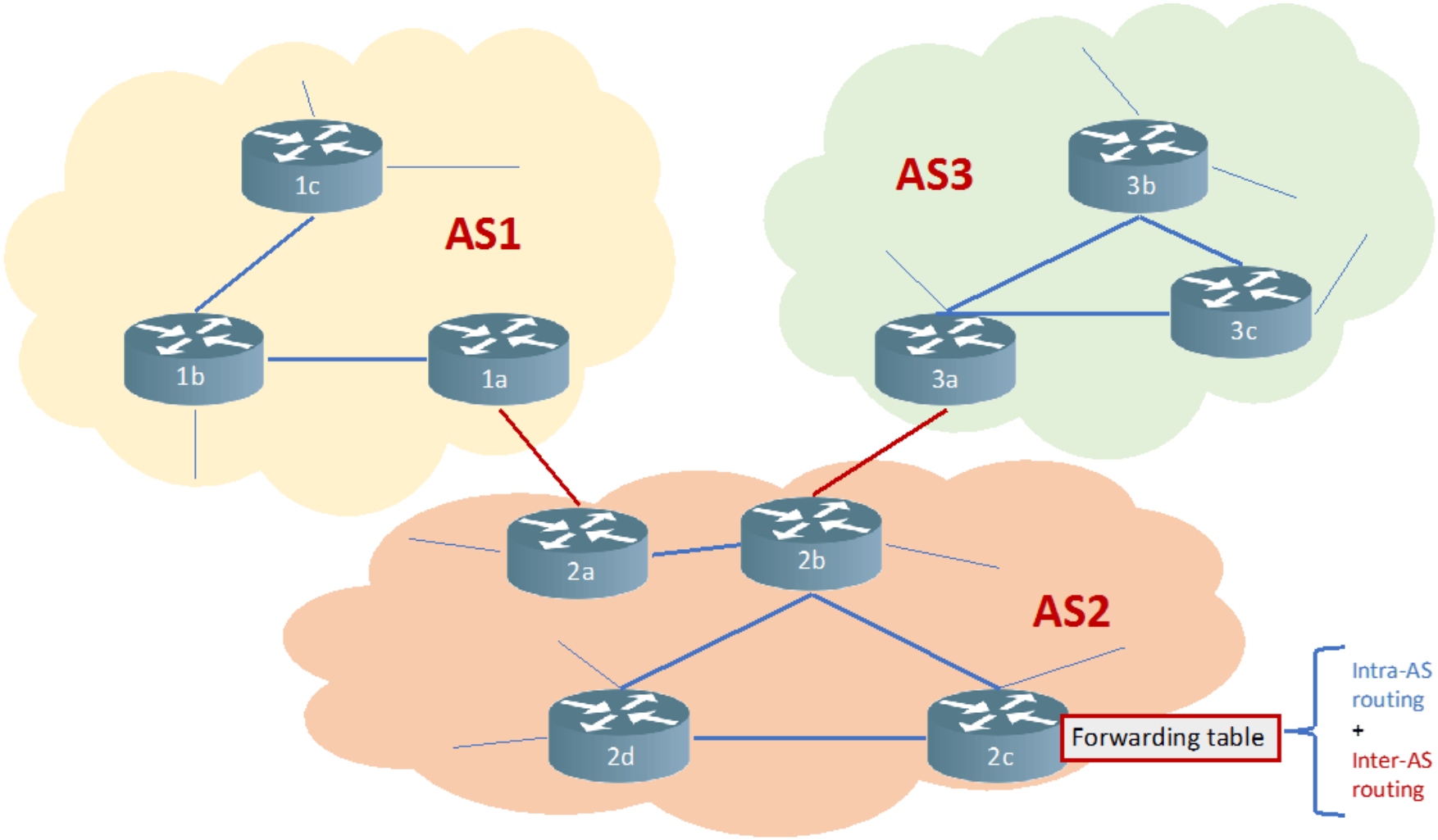


Figure 18 Example of three interconnected autonomous systems

This figure represents an example of three interconnected autonomous systems. AS1 is connected to AS2, and AS2 is connected to AS3.

Intra-AS routing: OSPF

Also known as interior gateway protocols (IGP)

Most common intra-AS routing protocols:

- RIP: Routing Information Protocol
- OSPF: Open Shortest Path First (IS-IS protocol essentially same as OSPF)

OSPF (Open Shortest Path First)

- It is “open”: publicly available
- Uses link-state algorithm
    - Link state packet dissemination
    - Topology map at each node
    - Route computation using Dijkstra’s algorithm
- Router floods OSPF link-state advertisements to all other routers in entire AS
    - Carried in OSPF messages directly over IP (rather than TCP or UDP)
    - Link state: for each attached link
- IS-IS routing protocol: nearly identical to OSPF

Inter-AS routing: BGP

BGP (Border Gateway Protocol): the de facto inter-domain routing protocol

- “glue that holds the Internet together”

BGP provides each AS a means to:

- eBGP: obtain subnet reachability information from neighboring ASes
- iBGP: propagate reachability information to all AS-internal routers.
- Determine “good” routes to other networks based on reachability information and policy

Allows subnet to advertise its existence to rest of Internet: “I am here”

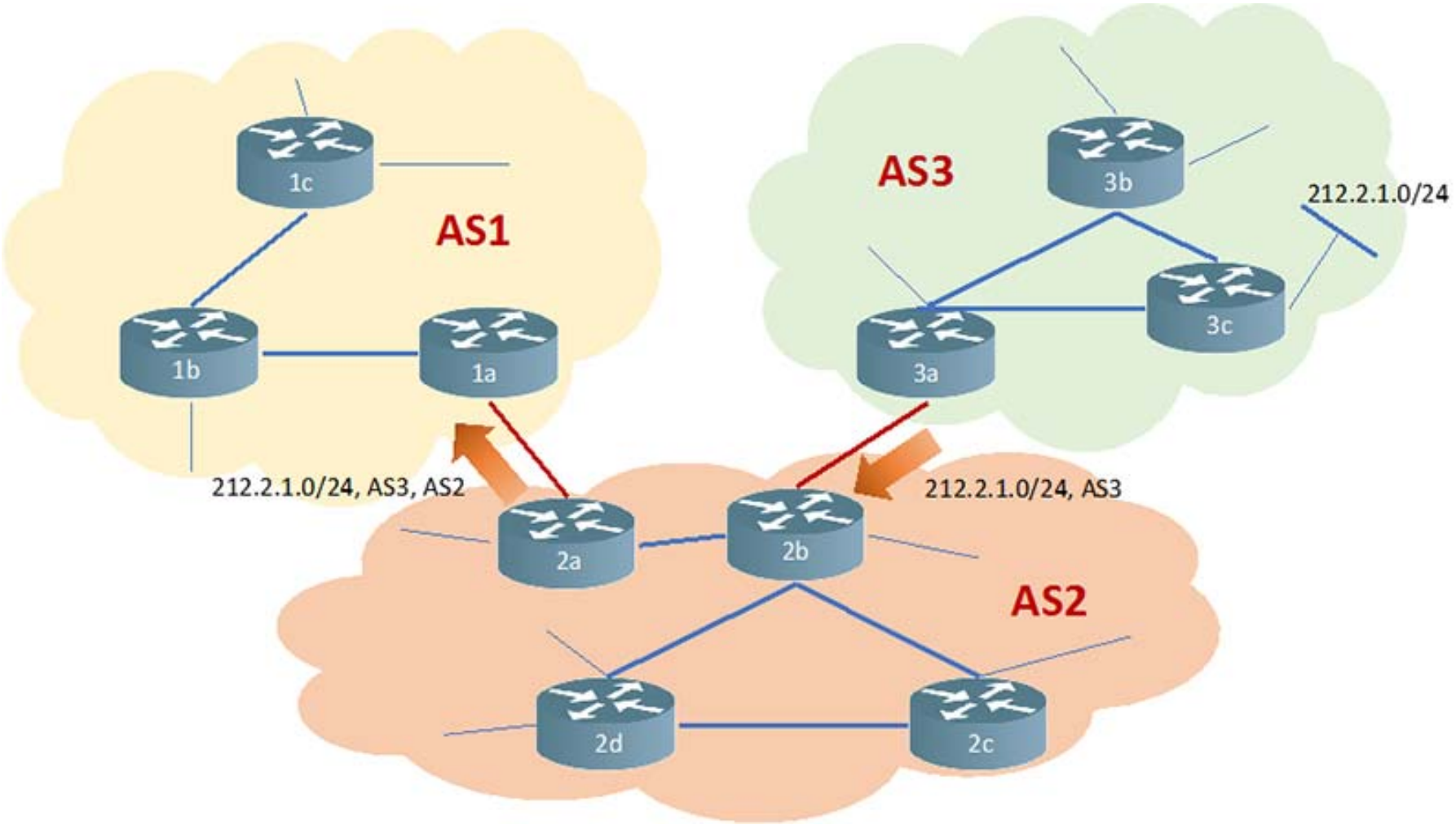


Figure 19 AS3 autonomous system advertises a subnet to AS2, and then AS2 advertises to AS1

ICMP: Internet control message protocol

Used by hosts & routers to communicate network-level information such as:

- Error reporting: unreachable host, network, port, protocol

Echo request/reply (used by ping)

ICMP can be seen as network-layer "above" IP:

- ICMP messages carried in IP datagrams
- ICMP message: type, code, plus first 8 bytes of IP datagram causing error

Type	Code	description
0	0	echo reply (ping)
3	0	dest. network unreachable
3	1	dest host unreachable
3	2	dest protocol unreachable
3	3	dest port unreachable
3	6	dest network unknown
3	7	dest host unknown
4	0	source quench (congestion control - not used)
8	0	echo request (ping)
9	0	route advertisement
10	0	router discovery
11	0	TTL expired
12	0	bad IP header

Figure 20 Type and Code fields in ICMP message

Network Management

Network management includes the deployment, integration and coordination of the hardware, software, and human elements to monitor, test, poll, configure, analyze, evaluate, and control the network and element resources to meet the real-time, operational performance, and Quality of Service requirements at a reasonable cost. Managed devices contain managed objects whose data is gathered into a Management Information Base (MIB):

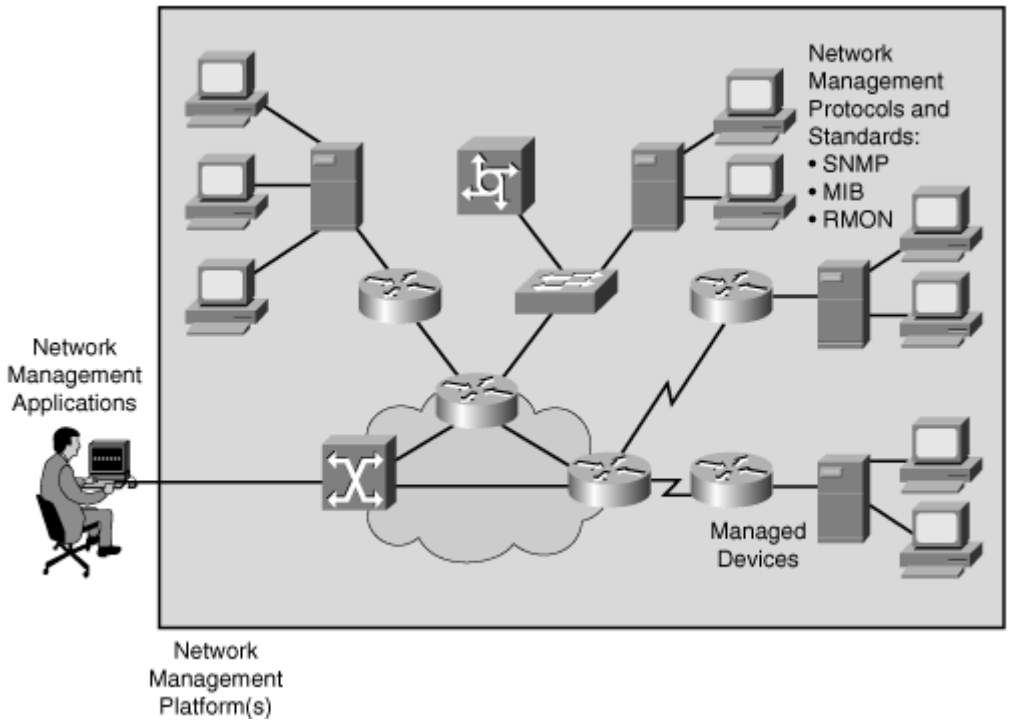


Figure 21 Example of network management infrastructure

The Simple Network Management Protocol (SNMP) defines request, response and trap commands:

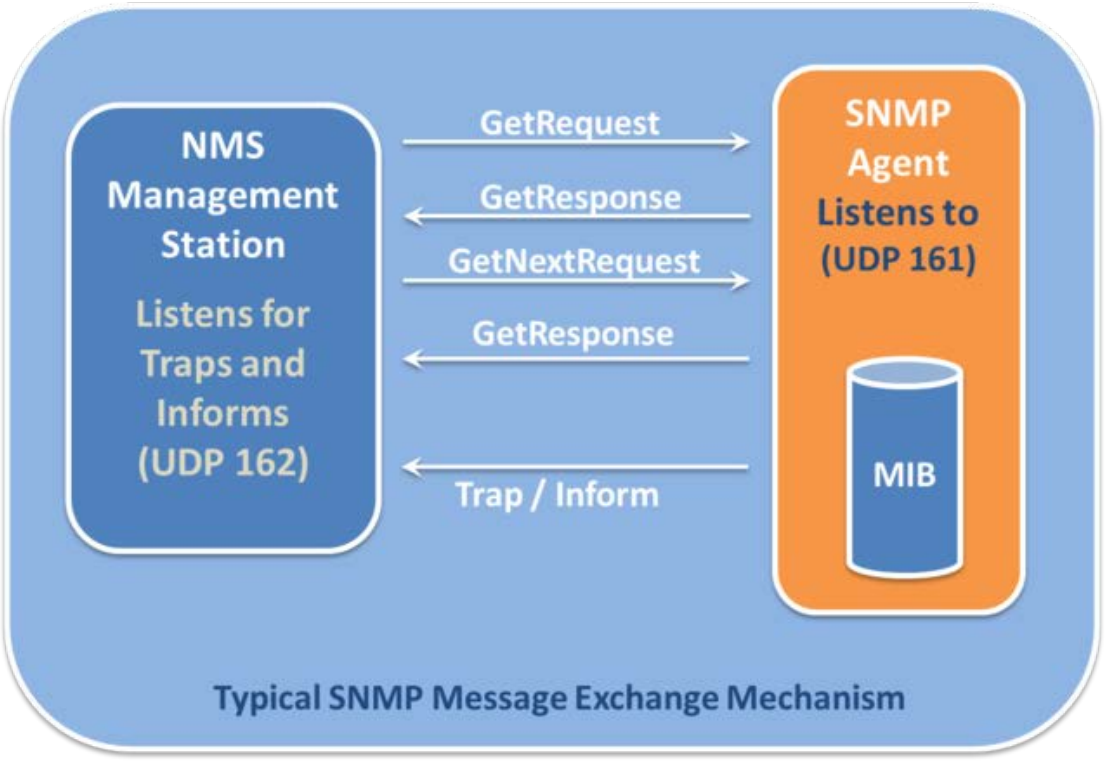


Figure 22 Typical SNMP message exchange mechanism

The link layer

Data-link layer has responsibility of transferring datagram from one node to physically adjacent node over a link. Links are communication channels that connect adjacent nodes along communication path. We may have wired, wireless links and LANs. Link layer packet is called frame, which encapsulates datagrams.

Which services may offer the link layer?

- Framing
- Reliability (usually implemented on transport layer, not in link layer)
- Flow control (usually implemented on transport layer, not in link layer)
- Error detection (parity bits, CRC, …)
- Error correction (FEC, …)
- Medium access control
- Addressing

Link layer is implemented in “adaptor” (network interface card NIC) or on a chip.

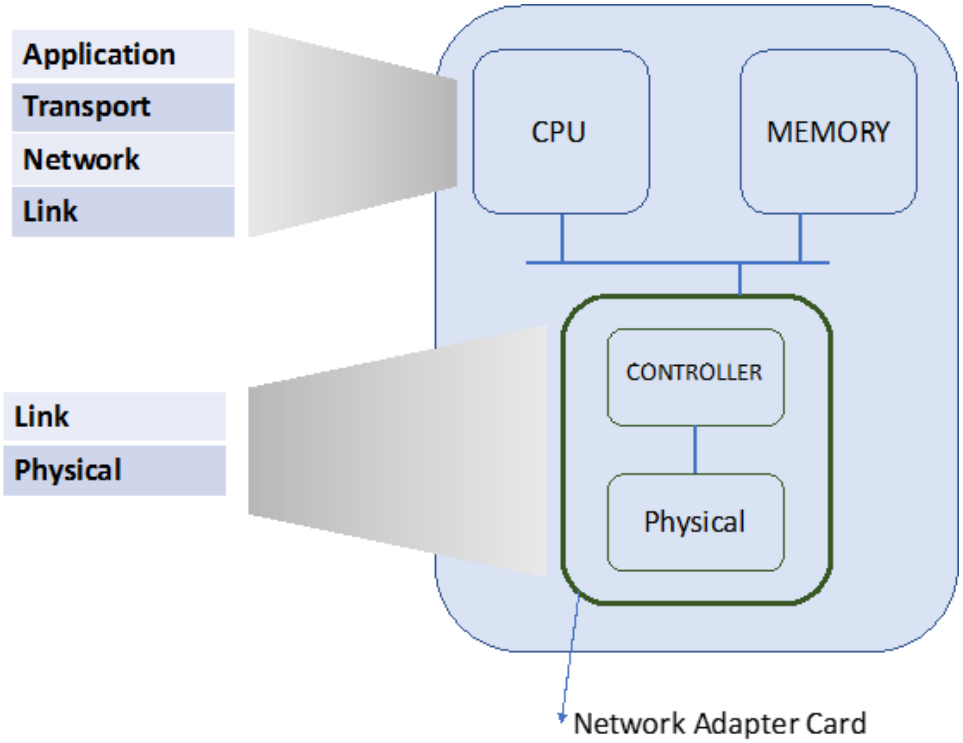


Figure 23 Network Adapter Card schema

Multiple access protocols

There are two types of links: point-to-point and broadcast (shared wire or medium). In single shared broadcast channel two or more simultaneous transmissions may collide. We need a multiple access protocol that determines how nodes share channel. An ideal multiple access protocol satisfies the following desiderata given a broadcast channel of R bps:

1. When one node wants to transmit, it can send at rate R.
2. When M nodes want to transmit, each can send at average rate R/M
3. Fully decentralized:
    a. No special node to coordinate transmissions
    b. No synchronization of clocks, slots
4. Simple

There are three broad classes of MAC (Medium Access Control) protocols:

- Channel partitioning: divide channel into smaller “pieces”, e.g. Frequency Division Multiplexing, Time Division Multiplexing
- Random access: MAC protocol specifices how to detect collisions and how to recover, e.g. ALOHA, slotted ALOHA, CSMA/CA
- Taking turns

Local Area Networks (LANs)

Each adapter on LAN has unique LAN address. A MAC, LAN, physical or Ethernet address is used “locally” to get frame from on interface to another physically-connected interface. Usually, 48 bit MAC address burned in NIC ROM, it does not change and it is portable, eg.: 2A-2B-1F-2C-93-53. However, IP hierarchical address is no portable, it depends on IP subnet to which node is attached.

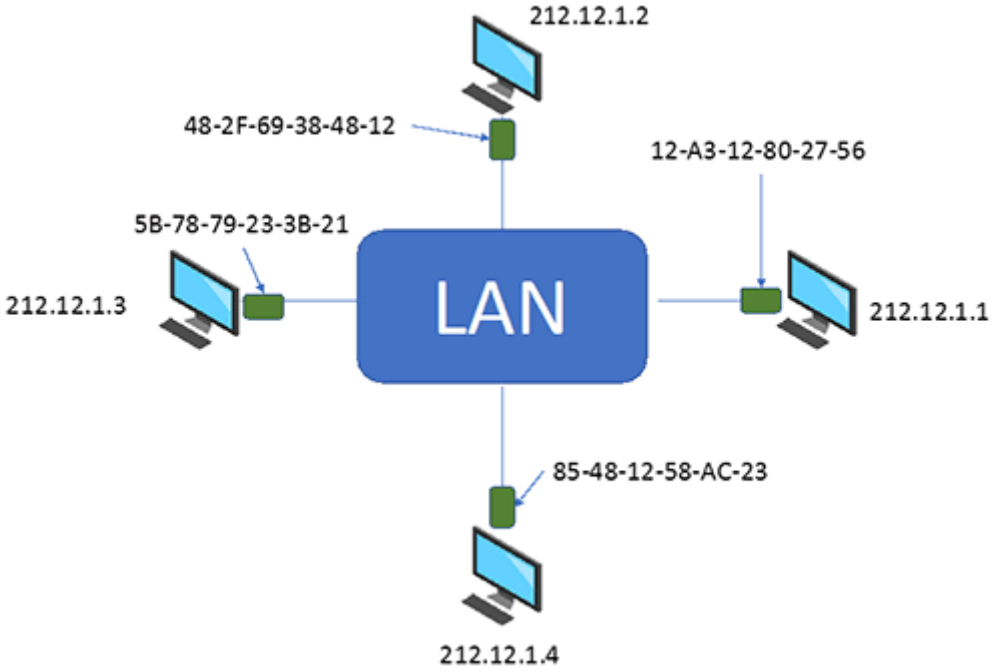


Figure 24 Example of LAN with IP and Ethernet addresses

ARP: address resolution protocol

How to determine interface's MAC address, knowing its IP address?

Using an ARP table: each IP node (host, router) on LAN has an ARP table with:

- IP/MAC address mappings for some LAN nodes: <IP address; MAC address; TTL>
    - TTL (Time To Live): time after which address mapping will be forgotten (typically 20 min)

How ARP works in the same LAN?

- A wants to send datagram to B
    - B's MAC address not in A's ARP table.
- A broadcasts ARP query packet, containing B's IP address
    - Destination MAC address = FF-FF-FF-FF-FF-FF
    - All nodes on LAN receive ARP query
- B receives ARP packet, replies to A with its (B's) MAC address
    - Frame sent to A's MAC address (unicast)
- A caches (saves) IP-to-MAC address pair in its ARP table until information becomes old (times out)

Ethernet

Dominant wired LAN technology, from 10Mbps to Gbps. Single chip, multiple speeds, simpler, cheap.

Sending adapter encapsulates IP datagram in Ethernet frame:

Figure 25 Ethernet frame format

An Ethernet frame has the following fields:

- Preamble: 7 bytes 10101010 followed by one byte 10101011.
- Addresses: 6 byte source, destination MAC addresses
- Type: indicates higher layer protocol (usually IP)
- CRC: cyclic redundancy check. If error detected, frame is dropped

Ethernet is connectionless and unreliable. There are many different Ethernet standards depending on different speeds and physical layer media.

Ethernet switch

An Ethernet switch is a link-layer device which stores and forwards Ethernet frames. It examines incoming frame's MAC address, selectively forwards frame to one-or-more outgoing links when frame is to be forwarded. Switches do not need to be configured, these are plug-and-play and self-learning devices. Self-learning switches can be connected together and perform as a unique switch.

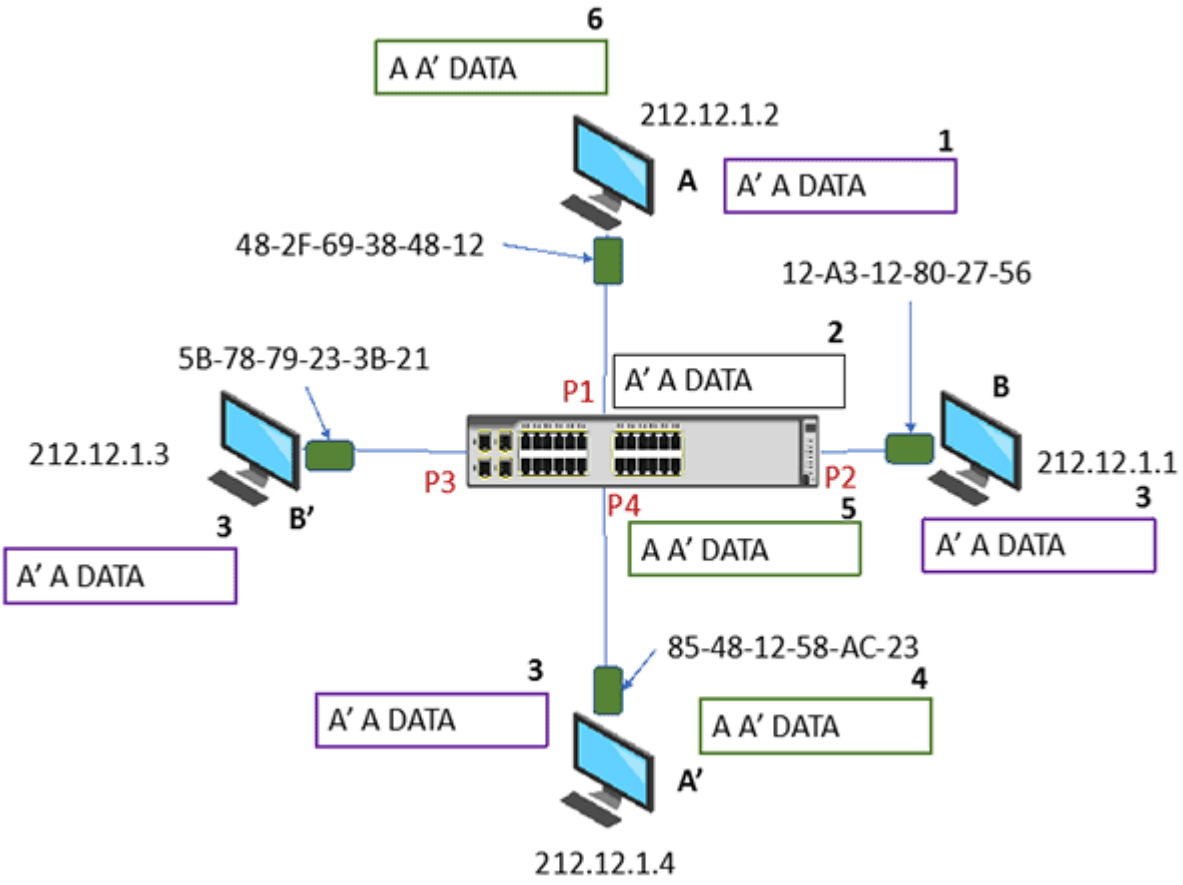


Figure 26 This is an example of self-learning in a switch. The switch table is initially empty.
A sends a frame to A'.
When switch receives frame A, it learns A-P1, then floods the ports. A' responds and then the switch learns A'-P4. In this case the switch selectively sends the response frame to port 1.

VLANs Virtual LANs

Switches supporting VLAN capabilities can be configured to define multiple virtual LANs over single physical LAN infrastructure.

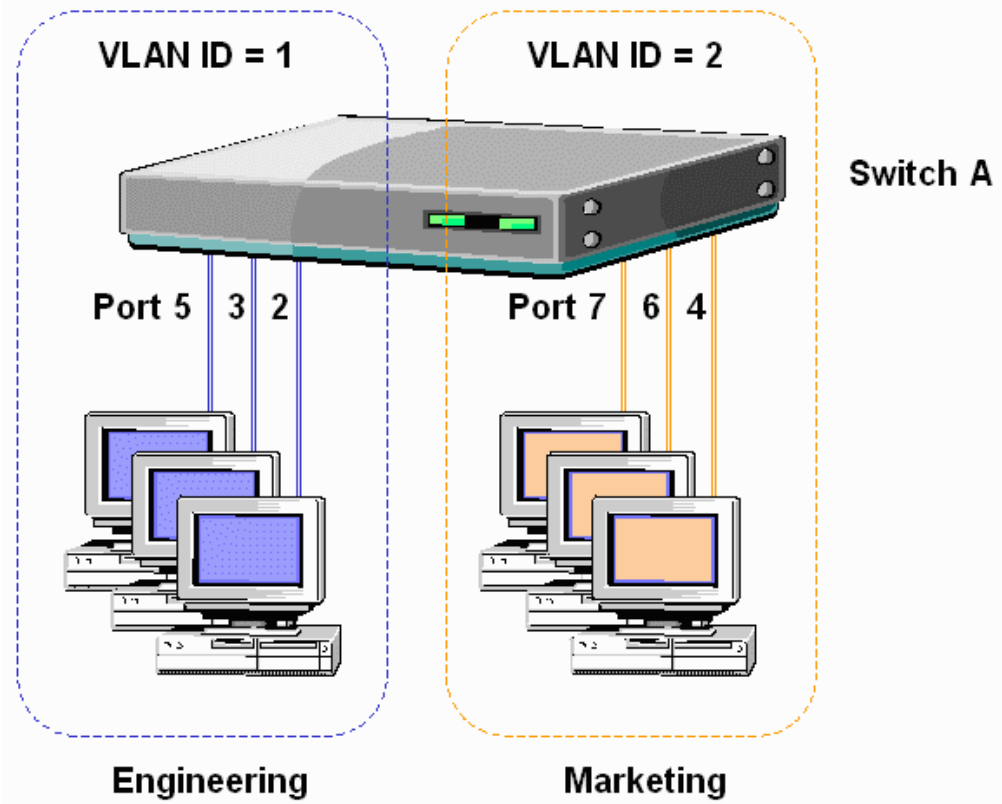


Figure 27 Example of a switch with two VLANs
Virtual LAN by Oyuhain (Own work) from Wikipedia CC BY-SA 4.0

We also may have VLANs spanning multiple switches:

Figure 28 Rackmount Ethernet switches and patch panels may build several VLANs
A couple of managed D-Link Gigabit Ethernet rackmount switches.... by Dsimic (Own work) from Wikipedia CC BY-SA 4.0

Trunk port carries frames between VLANs defined over multiple physical switches. Frames forwarded within VLAN between switches can't be vanilla 802.1 frames. 801.1q protocol adds/removes additional header fields for frames forwarded between trunk ports.

Wireless networks

Depending on the number of hops and the existence of an infrastructure we have the following wireless network taxonomy:

	SINGLE HOP	MULTIPLE HOPS
Infrastructure (Access point)	WiFi, WiMax, cellular: connect to base station to connect to Internet	Mesh networks: may have to relay through several wireless nodes to connect to Internet
No infrastructure	Bluetooth, Ad-hoc networks: There is no base station and connection to Internet	MANET, VANET: Relay to reach destination but no connection to Internet

Figure 29 Wireless Network taxonomy defined in terms of the number of hops and the existence of an infrastructure

Important differences from wired link …

- Decreased signal strength: radio signal attenuates as it propagates through matter (path loss)
- Interference from other sources: standardized wireless network frequencies (e.g., 2.4 GHz) shared by other devices (e.g., phone); devices (motors) interfere as well
- Multipath propagation: radio signal reflects off objects ground, arriving ad destination at slightly different times
- Hidden terminal problem: two or more stations connected to other station cannot hear each other

The figure below shows different wireless technologies in terms of distance and bitrate.

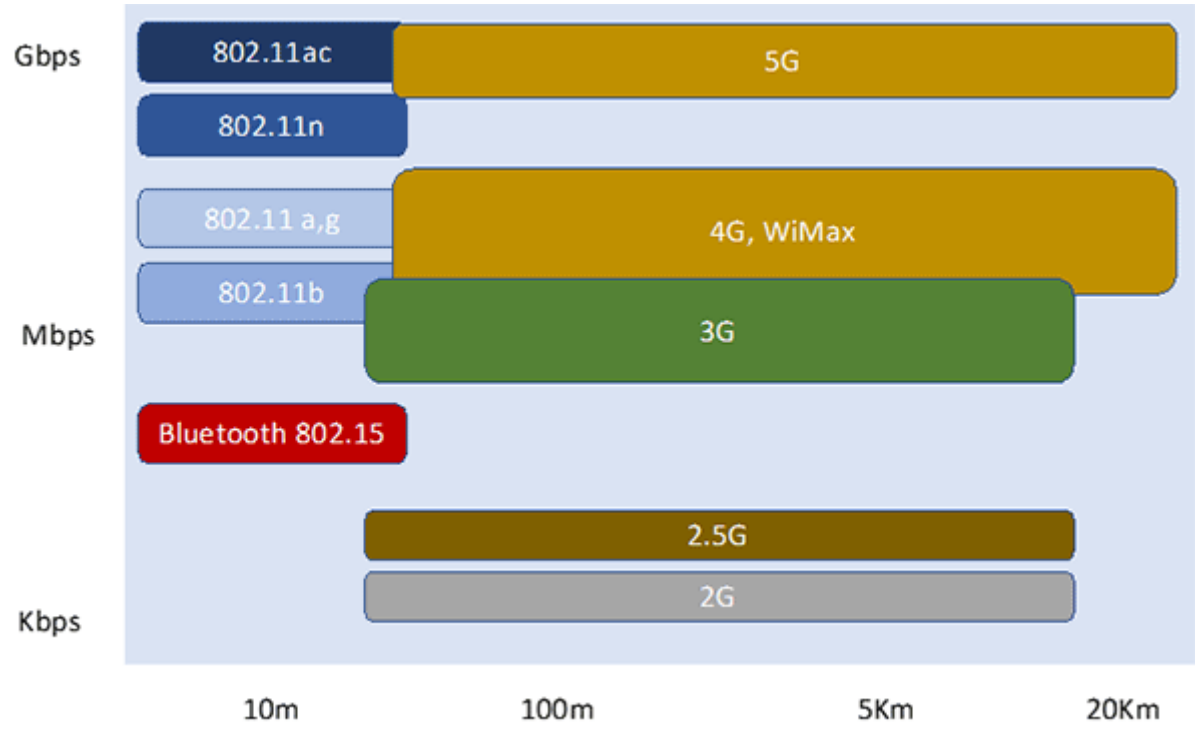


Figure 30 Distance vs bitrate for different wireless network technologies

IEEE 802.11 (WiFi)

Wireless host communicates with base station. A base station = access point (AP). In ad-hoc mode, hosts only. Different versions:

- …
- 802.11a
    - 5-6 GHz range, up to 54 Mbps
- 802.11g
    - 2.4-5 GHz range, up to 54 Mbps
- 802.11n: multiple antennae
    - 2.4-5 GHz range, up to 200 Mbps

All use CSMA/CA for multiple access, and all have base-station and ad-hoc network versions (without base-station). Spectrum divided into 11 channels at different frequencies

- Access point (AP) admin chooses frequency for AP
- Interference possible: channel can be same as that chosen by neighboring AP!

Host: must associate with an AP

- Scans channels, listening for beacon frames containing AP's name (SSID) and MAC address
- Selects AP to associate with
- May perform authentication
- Will typically run DHCP to get IP address in AP's subnet

IEEE 802.11: Multiple access

- Avoid collisions: two or more nodes transmitting at same time
- 802.11: CSMA - sense before transmitting
    - Don't collide with ongoing transmission by other node
- 802.11: no collision detection!
    - Difficult to receive (sense collisions) when transmitting due to weak received signals (fading)
    - Can't sense all collisions in any case: hidden terminal, fading
    - Goal: avoid collisions: CSMA/C(ollision)A(voidance)

IEEE 802.11: CSMA/CA

802.11 sender:

1. If sense channel idle for a time DIFS, then transmit entire frame (no CD)
2. If sense channel busy then start random backoff time timer counts down while channel idle transmit when timer expires. If no ACK, increase random backoff interval, repeat 2

802.11 receiver:

1. If frame received OK return ACK after a period of time SIFS (ACK needed due to hidden terminal problem)

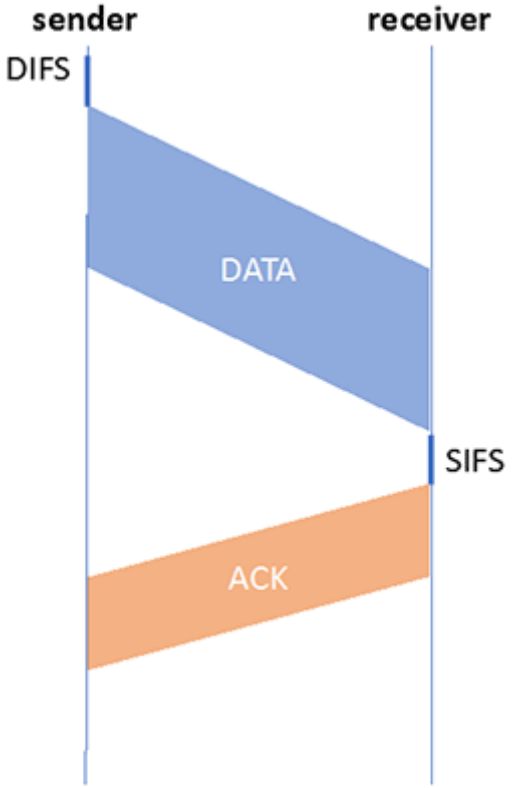


Figure 31 Data transmission in IEEE 802.11

In order to avoid collisions, allow sender to “reserve” channel rather than random access of data frames: avoid collisions of long data frames.

- Sender first transmits small request-to-send (RTS) packets to BS using CSMA
    - RTSs may still collide with each other (but they’re short)
- BS broadcasts clear-to-send CTS in response to RTS
- CTS heard by all nodes
    - Sender transmits data frame
    - Other stations defer transmissions

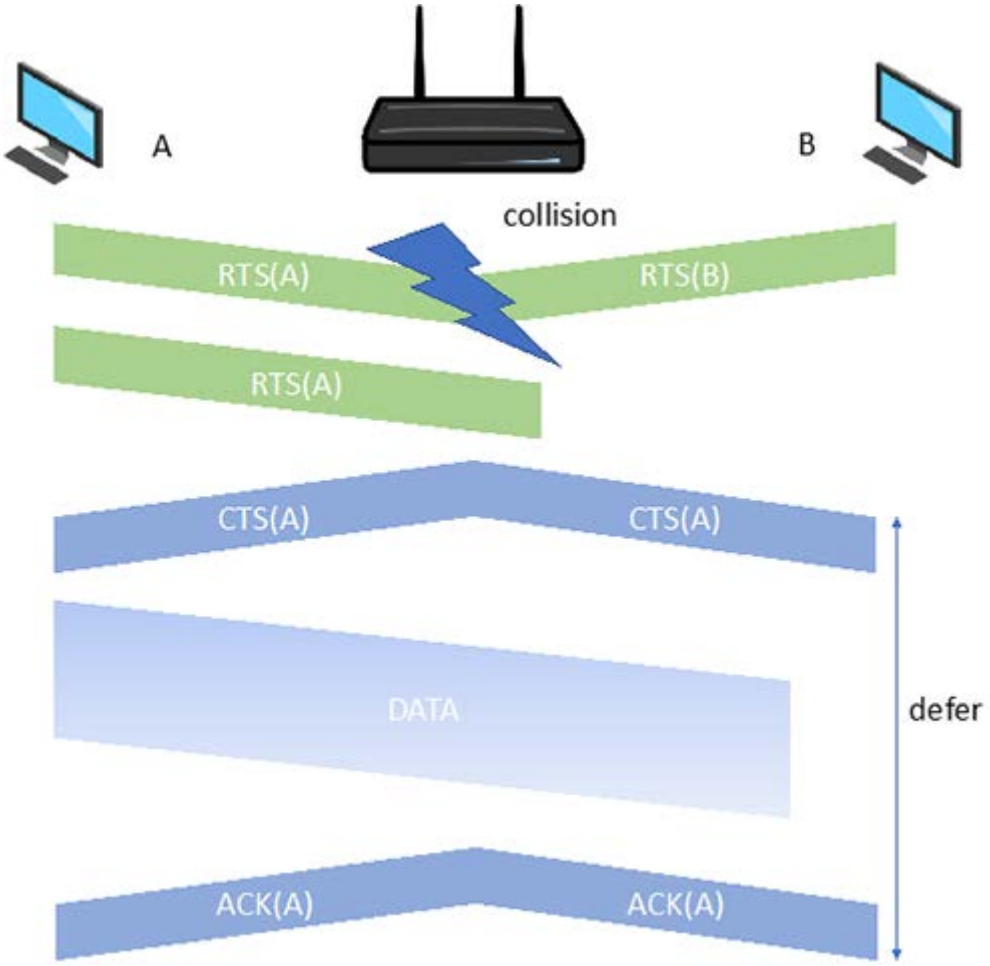


Figure 32 Data transmission in IEEE 802.11 using RTS and CTS

IEEE 802.11: Addressing

Next figure shows the data frame format in IEEE 802.11. As it can be seen, the frame contains four different address fields.

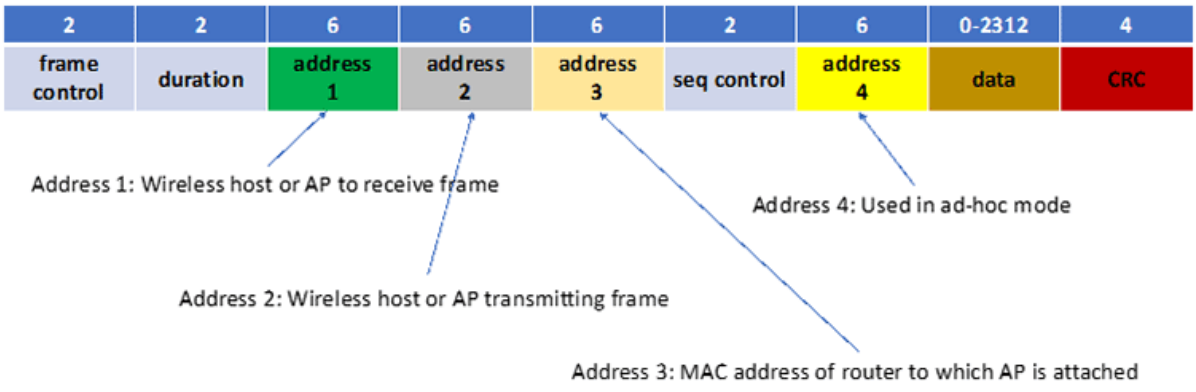


Figure 33 802.11 frame format

Address fields in IEEE 802.11 frame are used to distinguish among source, destination and routers.

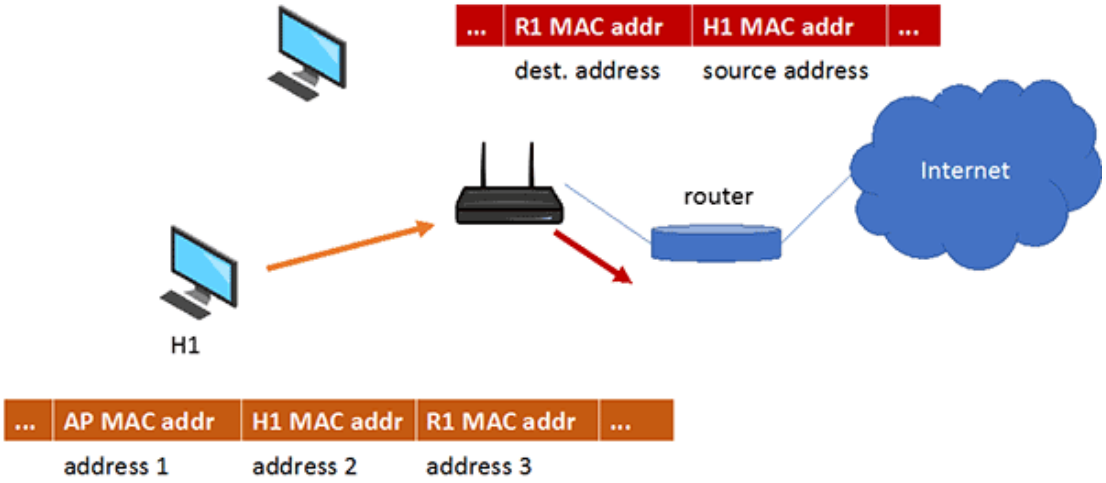


Figure 34 Frame formats when routing data from wireless LAN to the Internet

IEEE 802.15 Personal Area Networks

- Less than 10 m diameter
- Replacement for cables (mouse, keyboard, headphones)
- Ad hoc: no infrastructure
- Master/slaves:
    - Slaves request permission to send (to master)
    - Master grants requests
- 802.15: evolved from Bluetooth specification
    - 2.4-2.5 GHz radio band
    - Up to 721 kbps

Network security

The main network security concepts are:

- Confidentiality: only sender, intended receiver should “understand” message contents
    - Sender encrypts message
    - Receiver decrypts message
- Authentication: sender, receiver want to confirm identity of each other
- Message integrity: sender, receiver want to ensure message not altered (in transit, or afterwards) without detection
- Access and availability: services must be accessible and available to users

Principles of cryptography

In symmetric cryptography sender and receiver share a secret key. AES and DES are two Data Encryption Standards.

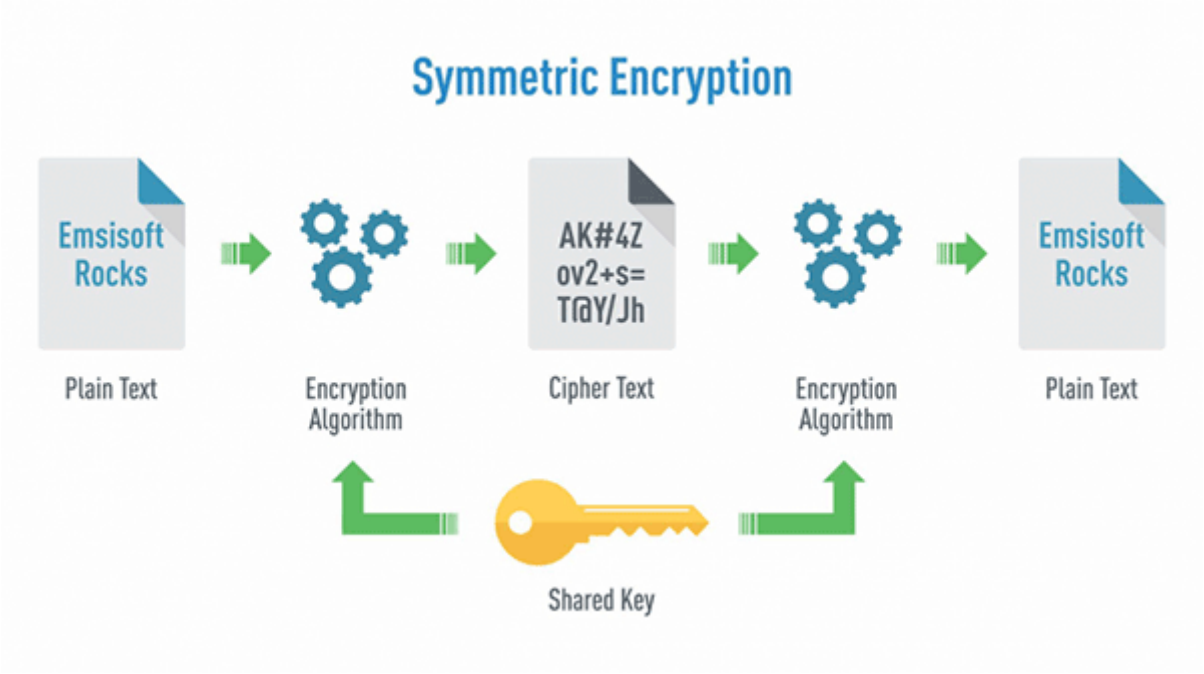


Figure 35 Symmetric Encryption schema
Симметрик түлхүүрийн шифрлэлт by Munkhzaya Ganbold (Own work)
from Wikipedia CC BY-SA 4.0

Public key cryptography (asymmetric encryption) is a radically different approach. Sender and receiver do not share secret key. Public encryption key known to all. Private decryption key known only to receiver.

Figure 36 Asymmetric Encryption schema
Simplified illustration of asymmetric/public key encryption... by Fleshgrinder and
The People from The Tango! Desktop Project... (Own work) from Wikipedia Public Domain

The sender needs the receiver's Public Key. The receiver owns a secret Private Key such that given the public key it should be impossible to compute private key. RSA (Rivest-Shamir-Adleman) algorithm was developed in 1977, and it is the most used public key cryptographic system.

However, RSA is computationally intensive. DES is at leas 100 times faster than RSA. In practice, we use public key crypto to establish secure connection, then establish second key symmetric session key for encrypting data. In the example, Bob and Alice use RSA to exchange a symmetric key Ks. Once both have Ks, they use symmetric key cryptography.

Message integrity and authentication

Digital signatures are a cryptographic technique analogous to hand-written signatures. Sender uses his/her private key to cypher the message. Receiver verifies message signed by Sender by applying Sender's public key to the message.

Receiver thus verifies that:

- Sender signed the message and no one else

Non-repudiation:

- Receiver can take the message and signature to court and prove that the Sender signed the message

Implementation of digital signature

It is computationally expensive to public-key-encrypt long messages. The goal is to have a fixed-length, easy to compute digital "fingerprint", and then to apply hash function H to m, get fixed size message digest, H(m). MD5 and SHA-1 are hash functions widely used.

Digital signature is a signed message digest:

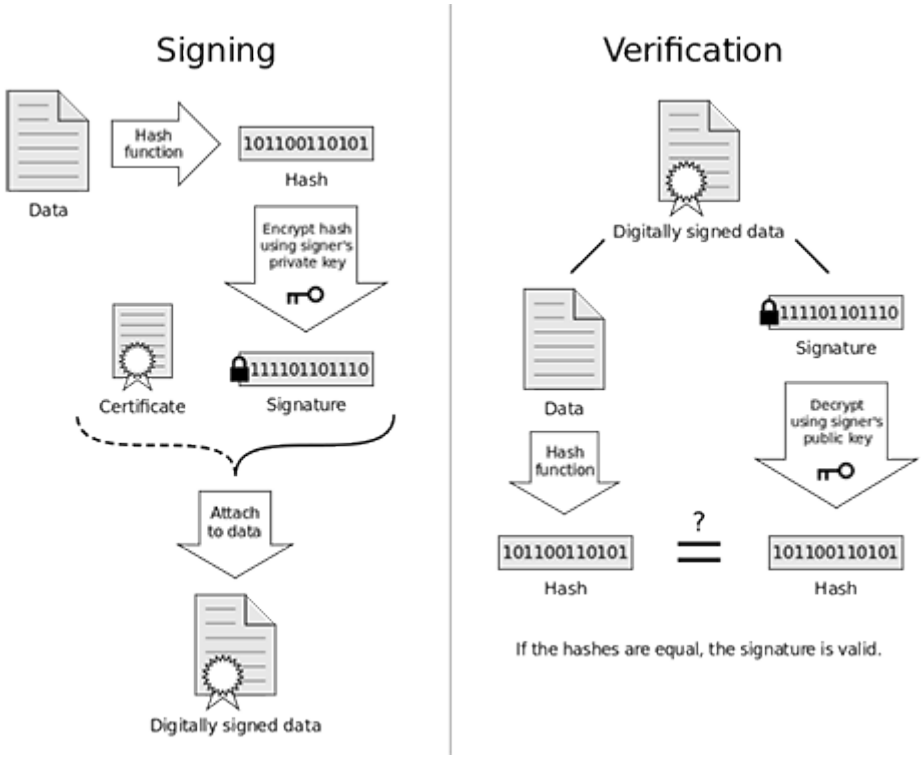


Figure 37 Operation of a digital signature and its verification
Diagram illustrating how a simple digital signature is applied and verified by Acdx (Own work) from Wikipedia CC BY-SA 3.0

Public-key certification

A certification authority (CA) binds public key to particular entity, E.

E (person, router) registers its public key with CA.

- E provides “proof of identity” to CA.
- CA creates certificate binding E to its public key.
- Certificate containing E’s public key digitally signed by CA – CA says “this is E’s public key”

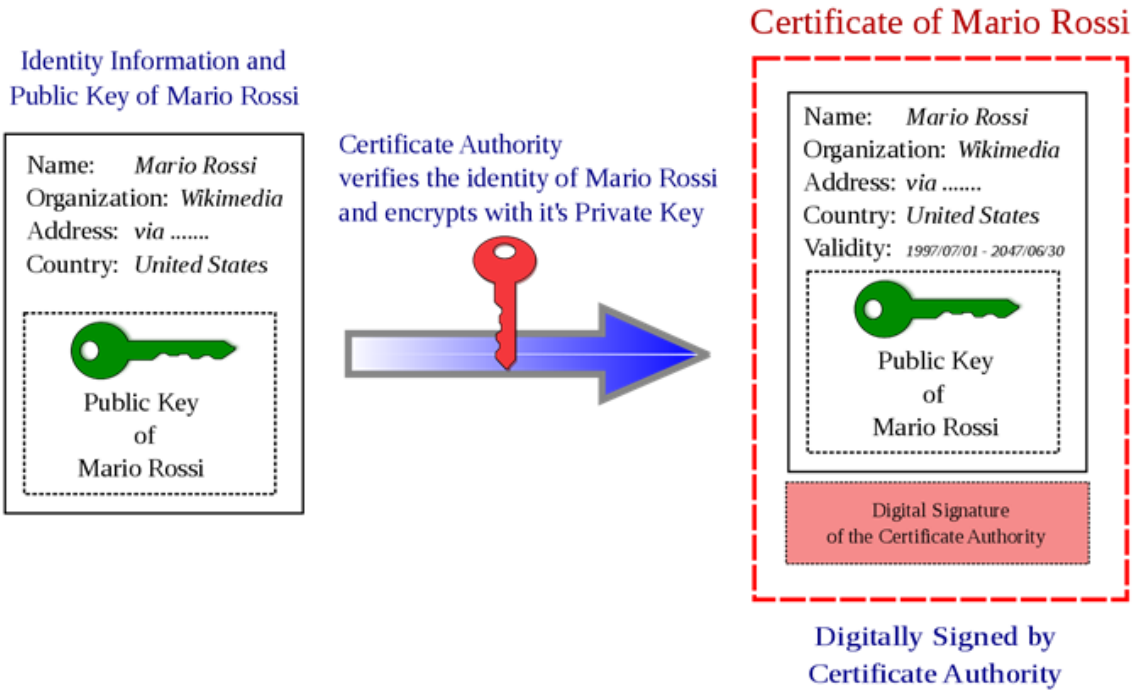


Figure 38 Operation of a certification authority to generate a certificate
Public Key Certificate Diagram (Italian Version) by derivative work: JBrewster... from Wikipedia CC BY-SA 3.0

Operational security: Firewalls

Isolates organization's internal net from larger Internet, allowing some packets to pass, blocking others:

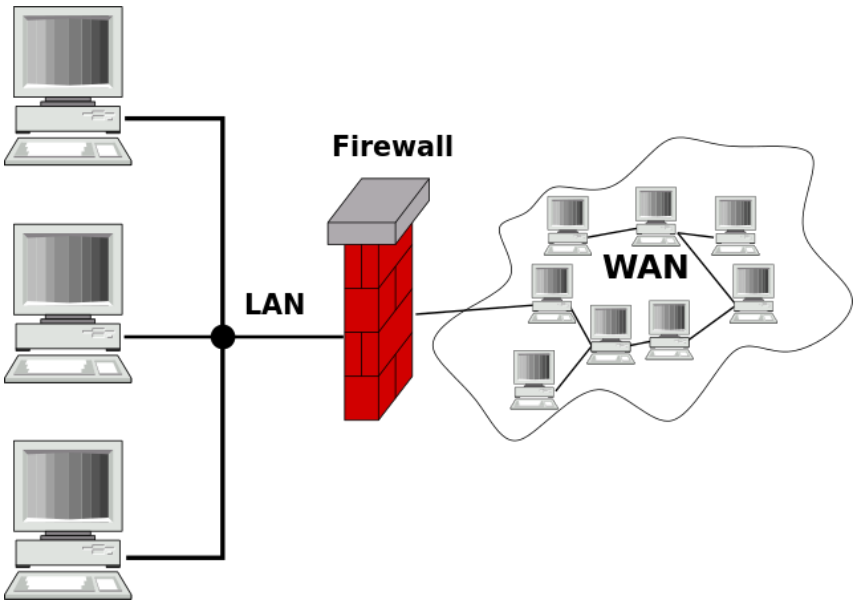


Figure 39 The firewall filters the flow of packets between the LAN and WAN
Gateway Firewall... by Harald Mühlböck... from Wikipedia CC BY-SA 3.0

Prevent denial of service attacks:

- SYN flooding: attacker establishes many bogus TCP connections, no resources left for “real” connections

Prevent illegal modification/access of internal data

- e.g., attacker replaces CIA’s homepage with something else
  Allow only authorized access to inside network
- Set of authenticated users/hosts

There are three types of firewalls:

- Stateless packet filters: decision to forward/drop packet based on source, destination IP address, TCP/UDP source and destination port numbers, ICMP message type and TCP SYN and ACK bits.
- Stateful packet filters: tracks status of every TCP connection to drop packets that “make no sense”. Basically, track connection setup (SYN), teardown (FIN).
- Application gateways: Filter packets on application data as well as on IP/TCP/UDP fields.

Intrusion detection systems

Packet filtering operates on TCP/IP headers only. IDS perform deep packet inspection, looking at packet contents (e.g., check characters strings in packet against database of known virus, attack strings). These also examine correlation among multiple packets: port scanning, network mapping, DoS attack.

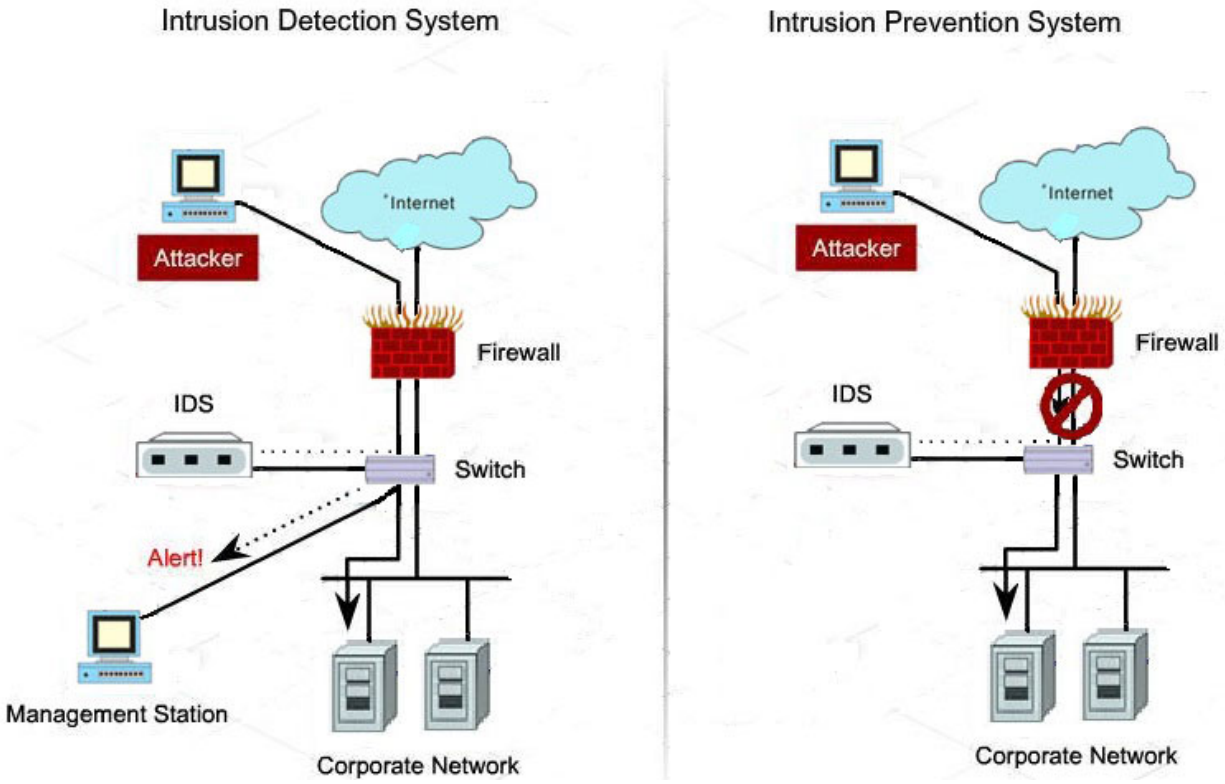


Figure 40 Example of intrusion detection systems to detect and prevent attacks intrusion prevention system by Чинбаатар - Own work from Wikipedia CC BY-SA 4.0

Further reading

J. Kurose & K.W. Ross. *Computer networking: A top-down approach*, 7th Ed., Pearson Education, 2017. Chapters 1, 4 to 8.