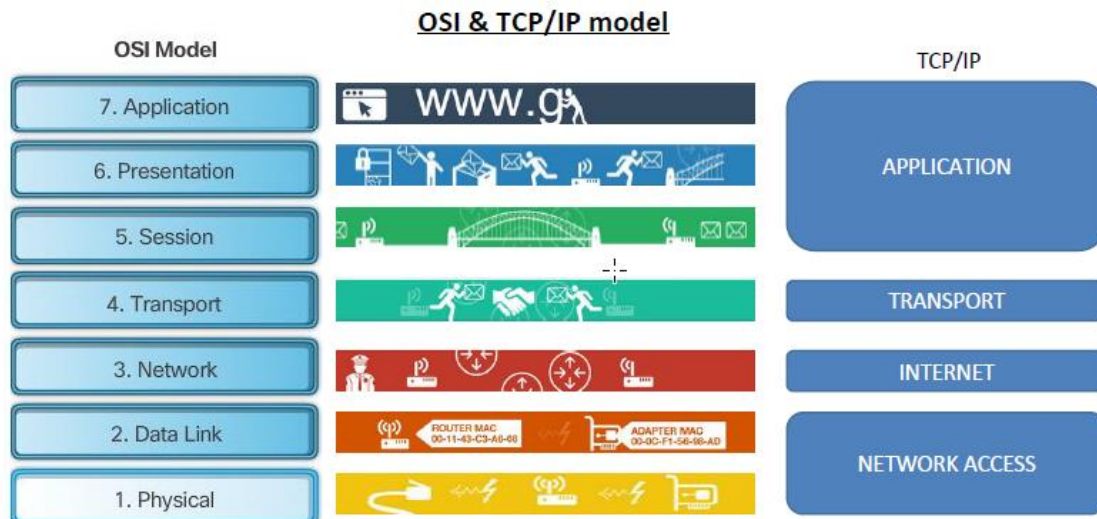


Chapter 1



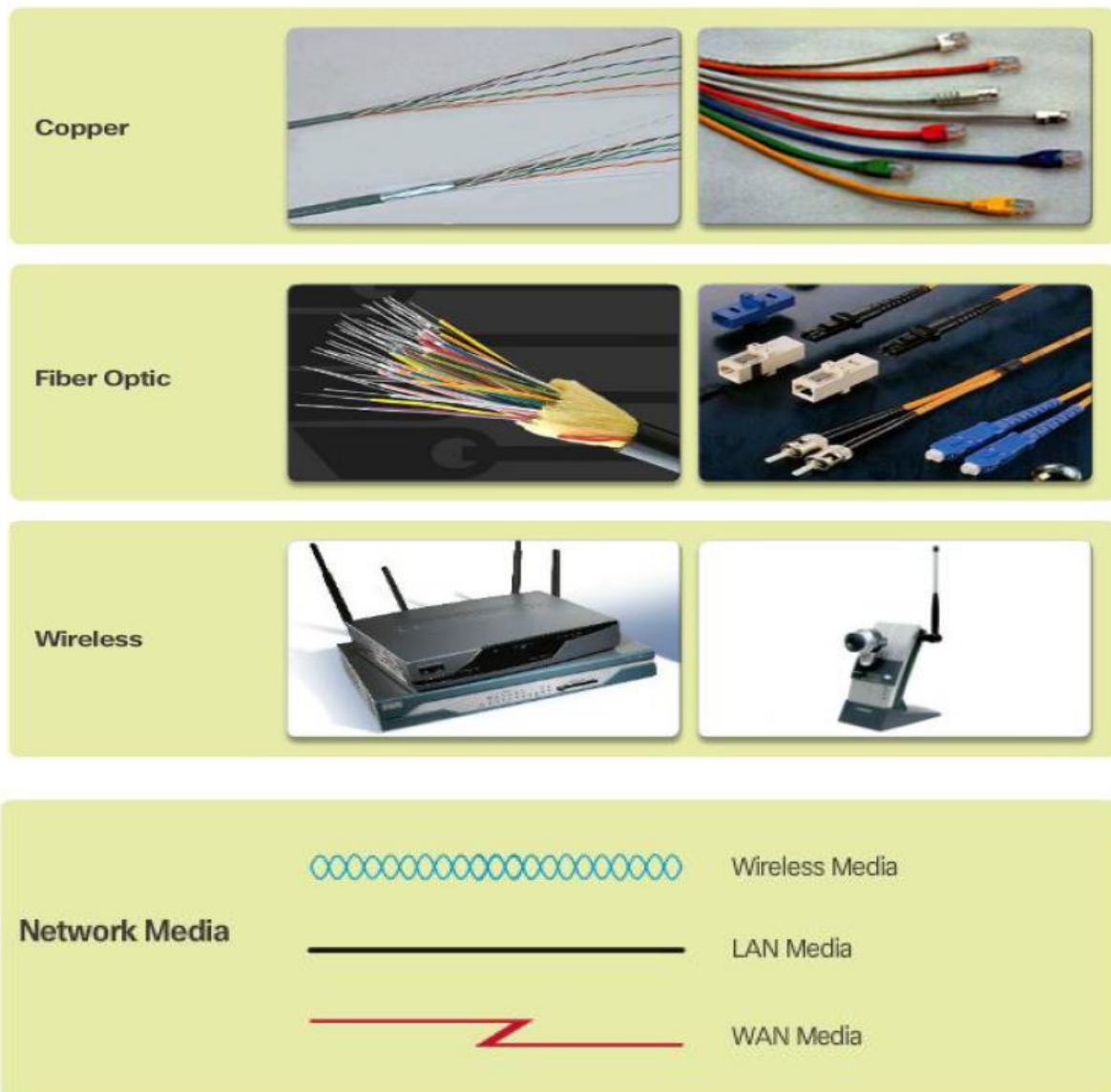
SOHO = Small Office – Home Office

Alle computers die verbonden zijn met een netwerk, worden hosts of end devices genoemd. Meestal zijn er dedicated servers maar soms is het handig om een computer tegelijk client en server te laten zijn. Dit noemt men peer-to-peer. De voordelen zijn gemakkelijk op te zetten, lage complexiteit, lage kost en voor simpele taken. De nadelen zijn geen gecentraliseerde administratie, niet erg veilig, niet uitbreidbaar en trage responsiviteit.

Devices zijn de apparaten op een netwerk, media zijn de kabels of de verbindingen tussen devices. Services zijn diensten die gehost worden op devices.



Soorten media:



Cable: Internet data signaal is over dezelfde kabel meegestuurd als televisie. Hoge bandbreedte en altijd beschikbaar.

DSL (Digital Subscriber Lines): loopt over een telefoonlijn (Asymmetrical DSL zorgt voor meer download- dan upload-snelheid) (Symmetric DSL zorgt voor evenveel upload als download)

Cellular: Overal beschikbaar, beperkt in mogelijkheden door gsm en zendmast

Satellite: Toegankelijk voor afgelegen gebieden, dishes moeten elkaar kunnen zien zonder obstakels

Dial-Up Telephone: lage bandbreedte, lage kosten, handig voor tijdens het reizen

Dedicated Leased Line: een deeltje huren van een grote optische fiberkabel, kan duur zijn

Ethernet WAN: verrijkt de LAN voordelen naar het WAN

LAN (Local Area Network) – WAN (Wide Area Network)

- Peer-To-Peer Netwerken
 - Voordelen
 - Gemakkelijk op te zetten
 - Weinig complex
 - Lagere kost
 - Kan voor simpele taken dienen zoals bestanden doorsturen of printers delen
 - Nadelen
 - Geen centrale administratie
 - Niet zo veilig
 - Niet scalable (uitbreidbaar)
 - Alle apparaten werken als server én client (kan de prestaties verminderen)
- Enkele termen
 - NIC = Network Interface Card (Lan adapter, netwerkkaart)
 - Physical Port = Netwerkpoot
 - Interface = Speciale porten op een router bv om met andere netwerken te verbinden
- Topologie
 - Physical Topology = Fysieke locaties identificeren (apparaten, poorten, kabels)
 - Logical Topology = Schema van IP-adressen/Poorten

Organisaties die helpen het Internet zijn structuur te behouden: IETF (Internet Engineering Task Force), ICANN (Internet Corporation for Assigned Names and Numbers), IAB (Internet Architecture Board) etc.

- internet (kleine i) = Meerdere netwerken met mekaar verbinden
- Internet (grote I) = World Wide Web

Intranet is een verzameling van LANs en WANs toegankelijk enkel voor werknemers en leden. Het extranet is toegankelijk voor mensen die niet in de organisatie werken, maar toch toegang nodig hebben. Het Internet is toegankelijk voor iedereen.

Een convergerend netwerk is een infrastructuur die de verschillende communicatiemogelijkheden samenbrengt in 1 medium. Ze kunnen data, geluid, beeld etc. over 1 connectie voortbrengen. Dit is in tegenstelling van een dedicated connection.

Een betrouwbaar netwerk kunnen we bepalen door een combinatie van factoren. Deze zijn fout-tolerantie, uitbreidbaarheid, beveiliging en Quality of Service (QoS).

- Fout-tolerantie: het Internet moet altijd beschikbaar blijven, ook als 1 route of onderdeel faalt. De oplossing is redundancy inbouwen. De gebruiker heeft hier geen weet van. Een uitzondering hierop is VoIP. Er wordt een dedicated connectie gemaakt en als die faalt moeten gebruikers herverbinden op een nieuwe manier.
- Uitbreidbaarheid: men moet het systeem altijd kunnen uitbreiden zonder dat het bestaande systeem hier nadelen van ondervindt.
- Quality of Service (QoS): het is een basis-principe voor het tegengaan van congestion en zorgt voor betrouwbare connecties voor gebruikers. Congestion gebeurt wanneer er meer bandbreedte opgevraagd wordt, dan beschikbaar. Als iemand streamt zal dit voorrang hebben op iemand die een website wil bekijken. De pakketten van de stream hebben voorrang.
- Beveiliging: er zijn algemeen 2 onderdelen hierbij nl. infrastructuur beveiliging en informatie beveiliging. Het is belangrijk apparaten ook fysiek te beveiligen naar softwarematig. Er zijn 3

factoren die alles bepalen nl. vertrouwelijkheid (geautoriseerde gebruikers kunnen alleen lezen en/of schrijven), integriteit (de zekerheid dat de data niet gemodificeerd is in de weg naar de gebruiker) en beschikbaarheid (de data moet beschikbaar zijn voor de gebruikers).

Netwerk-trends:

- Bring Your Own Device (BYOD): End-users brengen meer en meer hun eigen apparaten overal mee.
- Online samenwerking: Online samenwerking is de manier op direct en onmiddellijk contact te nemen met anderen terwijl ze niet in de buurt zijn.
- Video-communicatie: Mensen die op totaal verschillende plaatsen zijn kunnen elkaar en documenten live delen.
- Cloud computing: Alle bedrijven moeten hun data in een cloud opslagen. Dit kan door een eigen data-center te maken of door een deeltje te huren. We kunnen ook nog eens het onderscheid maken tussen een privé, publieke, hybride of costum cloud.

Netwerk-trends beïnvloeden ook onze huis-situatie. Dit noemt men Smart Home Technology. Men wil alle apparaten met elkaar laten communiceren. Powerline is het versturen van data over een stroom-connectie. Er moeten dan geen speciale datakabels geïnstalleerd worden.

DSL en kabel zijn de gewoonlijke manieren om een huis met het Internet te verbinden. Men kan ook voor een draadloze connectie kiezen. Wireless Internet Service Provider (WSIP) is een ISP dat door draadloze technologie met zijn gebruikers communiceert. Een andere draadloze optie is Wireless Broadband Service die gebruik maakt van mobiel internet zoals je op je gsm terugvindt.

Er zijn altijd beveiligingsrisico's maar men moet mogelijk zijn het netwerk te beveiligen en QoS zeer goed te houden. De beveiliging van een netwerk houdt het beheer van protocollen, technologieën, apparaten, tools en technieken in. Veel externe dreigingen zijn verspreid over het Internet.

- Virussen, wormen en Trojaanse paarden: Malware dat een speciale code laat uitvoeren bij de gebruikers.
- Spyware en adware: verzamelt stiekem informatie over de gebruiker.
- Zero-day aanvallen of zero-our aanvallen: een aanval dat gebeurt op de eerste dag dat een kwetsbaarheid bekend wordt.
- Hacker attacks: een aanval door een bewuste persoon op een end-device of netwerk-bronnen
- Denial of service aanvallen (DOS): aanvallen gemaakt om applicaties, processen of apparaten te vertragen.
- Data onderschepping en diefstal: aanval op privédata te stelen van een bedrijf of persoon
- Indentiteitsdiefstal: een aanval om de login-gegevens te stelen zodat men aan privédata kan.

Het is ook belangrijk aan interne dreigingen te denken. Dit wordt alsmaar belangrijker door BYOD.

Er is geen éénduidige oplossing voor deze problemen. Voor deze reden zou beveiliging over meerdere lagen gespreid moeten zijn. Als er 1 laag faalt dan zullen de andere alsnog mensen met foute bedoelingen buiten houden. Het minimum is antivirus- en antispysware-software en firewall filtering. In additie kunnen volgende onderdelen toegevoegd worden: Dedicated firewall systemen, Access Control Lists (ACL), intrusion prevention systems (IPS), Virtual Private Network (VPN).

Chapter 2

Het besturingssysteem van een netwerk-apparaat wordt een network operating system genoemd. Het deel dat rechtstreeks in praat met de hardware noemt men de kernel. Het deel dat praat tussen de software en de gebruiker is de shell (CLI & GUI). De OS van Cisco heet IOS.

Verbindingsmethoden:

- Console: wanneer je de router moet instellen als er nog geen netwerk-services geconfigureerd zijn.
- SSH: beveiligd verbinden.
- Telnet: onbeveiligd verbinden.
- AUX: er is geen verbinding mogelijk en je moet via een telefoon-verbinden van op afstand verbinden.

Router Modes:

| | | |
|-----------------------------|---------------------------|--|
| Router> | User mode | Limited to basic monitoring commands |
| Router# | Privileged mode (exec) | Provides access to all other router commands |
| Router(config)# | global configuration mode | Commands that affect the entire system |
| Router(config-if)# | interface mode | Commands that affect interfaces |
| Router(config-line)# | line mode | Commands that affect in lines modes (console, vty, aux...) |

Commando's



| | |
|------------------------------------|---|
| hostname # | veranderd de hostname van de switch naar # |
| enable | van User Exec Mode naar Privileged Exec Mode |
| disable | Van Privileged Exec Mode naar User Exec Mode |
| configure | |
| enable secret # | |
| enable password # | |
| show | |
| show version | Informatie over de software/hardware van het apparaat |
| show flash | Informatie over het flashgeheugen |
| show interfaces | Informatie over alle netwerk interfaces |
| show interfaces fastethernet 0/1 | (specifieke interface) |
| show processes | Informatie over alle processen |
| show cdp neighbors | Info over cisco apparaten die in de buurt zitten (cisco discovery protocol) |
| show arp | Informatie over de ARP-tabel (address resolution protocol: mac -> ip) |
| show mac-address-table | Info over de mac-adressen tabel (mac -> portnumbers) |
| show vlan | Info over de virtual lans(virtuele netwerken in het fysieke netwerk) |
| ? | geeft help |
| ip address # # | geeft ip het adres # met subnetmask # |
| no shutdown | veranderd de staat naar up of running |
| banner motd \$ ### \$ | zet de message of the day |
| copy running-config startup-config | de huidige config wordt na het opnieuw opstarten behouden |
| exit | 1 laag terug |
| end | terug naar Privileged Exec Mode |
| service password-encryption | zet encrypted password aan |
| reload | herstart de router |
| erase # | verwijdert het bestand # |

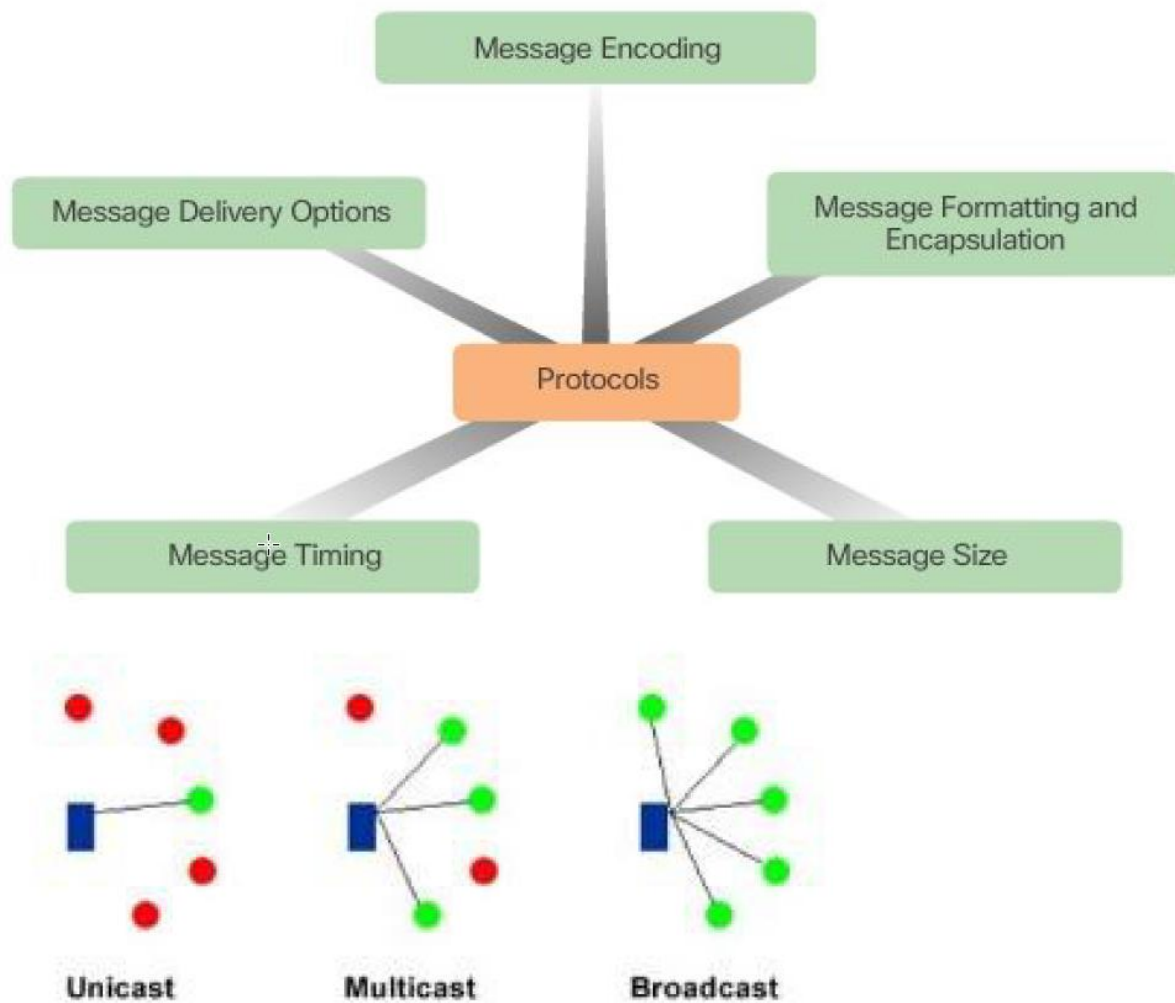
- **Ctrl-Shift-6** – Allows the user to interrupt an IOS process such as ping or traceroute.

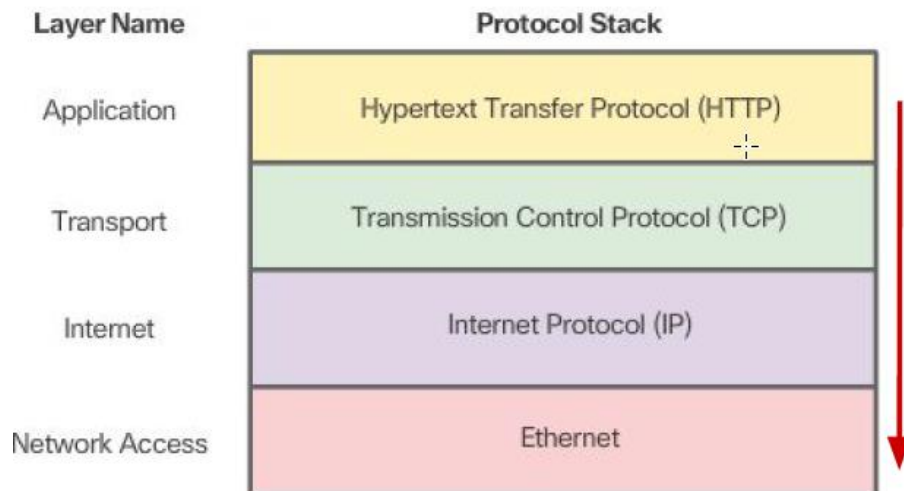
Guidelines to Choose a Hostname

- Start with a letter
- Contain no spaces
- End with a letter or digit
- Use only letters, digits and dashes
- less than 64 characters

Chapter 3

| | | | | | | |
|--|---|--|--|----------------------------------|-----------------------------|---|
| Destination (physical / hardware address) | Source (physical / hardware address) | Start Flag (start of message indicator) | Recipient (destination identifier) | Sender (source identifier) | Encapsulated Data (bits) | End of Frame (end of message indicator) |
| Frame Addressing | | Encapsulated Message | | | | |



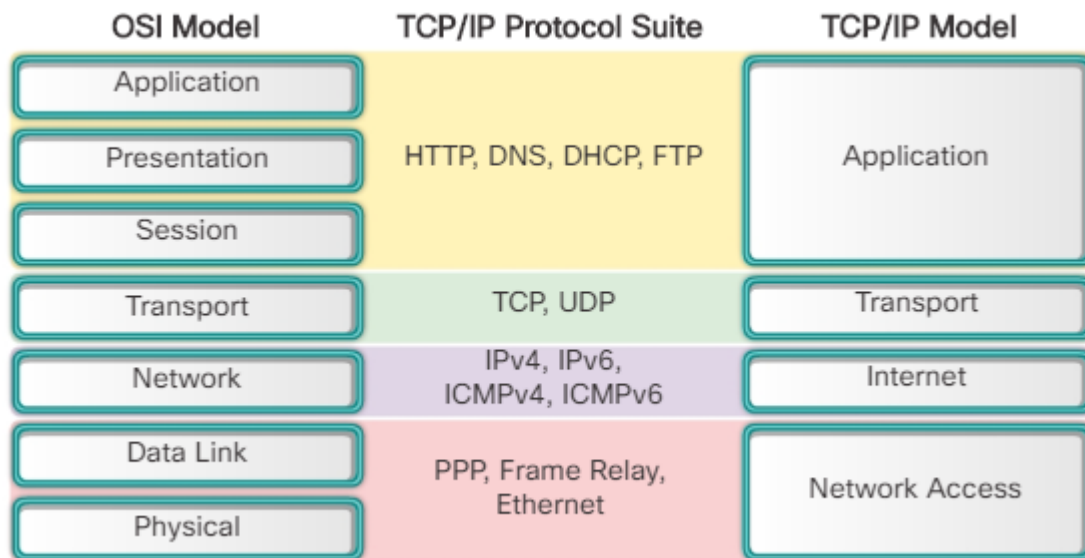



| Layer Name | TCP/IP | ISO | AppleTalk | Novell Netware |
|----------------|-----------------------------------|------------------------------|---------------------|----------------|
| Application | HTTP DNS DHCP FTP | ACSE ROSE TRSE SESE | AFP | NDS |
| Transport | TCP UDP | TP0 TP1 TP2 TP3 TP4 | ATP AEP NBP RTMP | SPX |
| Internet | IPv4 IPv6 ICMPv4 ICMPv6 | CONP/CMNS CLNP/CLNS | AARP | IPX |
| Network Access | Ethernet PPP Frame Relay ATM WLAN | | | |

Protocollen:

| | | |
|-------|-------------------------------|---|
| DNS | Domain Name System | vertaald namen naar IP's |
| BOOTP | Bootstrap Protocol | verkrijgt zelf zijn eigen IP, verstuurd een bestand voor boot |
| DHCP | Dynamic Host Configuration Pr | geeft dynamisch IP's |
| SMTP | Simple Mail Transfer Protocol | client naar server en server naar server (verzenden) |
| POP | Post Office Protocol | binnenhalen van mails (na ontvangen -> mail weg van server) |
| IMAP | Internet Message Access Pr | bekijken van mails op de server |
| FTP | File Transfer Protocol | ontvangen en verzenden van bestanden |
| TFTP | Trivial FTP | simpeler dan FTP, minder overhead |
| HTTP | Hypertext Transfer Protocol | Ontvangen van data op het WWW |
| TCP | Transmission Control Pr | ontvangsbevestiging nodig (belangrijke dingen) |
| UDP | User Datagram Protocol | geen ontvangstbevestiging (streaming) |
| IP | Internet Protocol | ontvangt segmenten en verpakt ze in pakketten |
| NAT | Network Address Translation | IP private -> IP public |
| ICMP | Internet Control Message Pr | waarschuwt host als er corrupte pakketten aankomen |

| | | |
|-------------------|--|--|
| OSPF | Open Shortest Path First | routing protocol (locatie) |
| EIGRP | Enhanced Interior Gateway Routing Protocol | routing protocol van Cisco (locatie, delay, betrouwbaarheid) |
| ARP | Address Resolution Protocol | komt MAC adressen van IP's te weten |
| PPP | Point-to-Point Protocol | encapsulatie van pakketten voor over seriële kabel |
| Ethernet | | bepaalde regels voor signaling standaarden en Netw Acc Layer |
| Interface Drivers | | instructie voor de controle van een interface op netwerk |





 All

 People

 Seem

 To

 Need

 Data

 Protocols



- Protocols used for process-to-process communications
- Application data
- PDU: Data



- Data representation
 - different computers might have different representations of characters
 - eg. ASCII vs EBCDIC
- Data compression (image, audio, video)
- Data encryption
- PDU: Data



- Service to presentation
- Controls the dialogues and data exchange
- Interhost communication
- establishes, manages and terminates sessions between the local and the remote application
- eg. cookie session and php session
- PDU: Data



- transfer, and reassemble the data for individual communications between the end devices.
- End-to-end communication and reliability
- services to segment
- Ports
- TCP, UDP segments
- PDU: Segment



- “services to exchange the individual pieces of data over the network between identified end devices”
- path determination
- Logical addressing
- IP address
- Router
- IP packet
- PDU: Packet



- Methods for exchanging data frames between devices over a common media.
- Physical addressing
- MAC address
- Switch
- Ethernet frames
- PDU: Frame



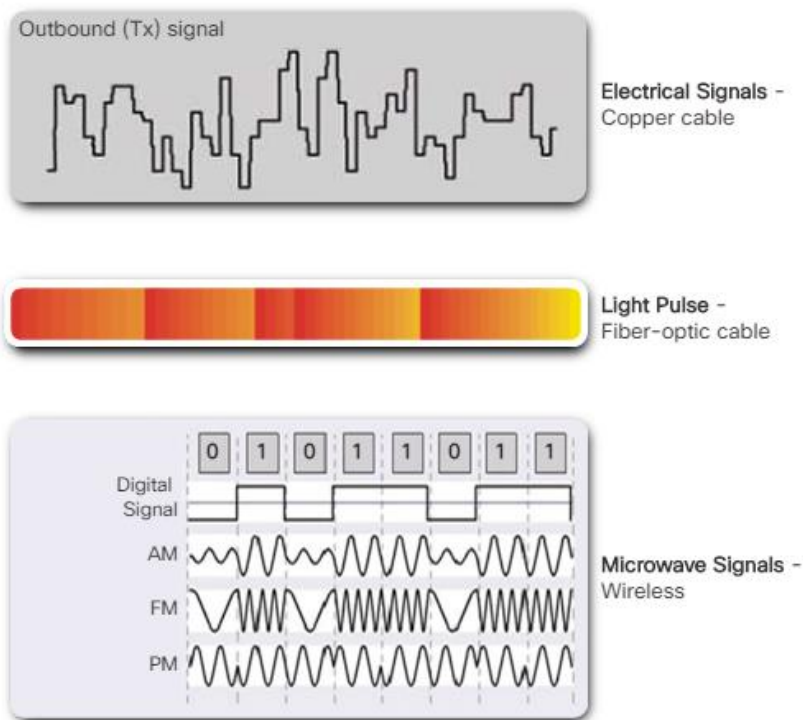
- mechanical, electrical, functional
- physical connections
- transmitting bits (to and from a network device)
- PDU: Bit

Segmentatie: de data in kleinere deeltjes onderverdelen en dan verzenden.

Multiplexing: elke gebruiker krijgt een deeltje van de bandbreedte, ieder wordt om de beurt data gegeven.

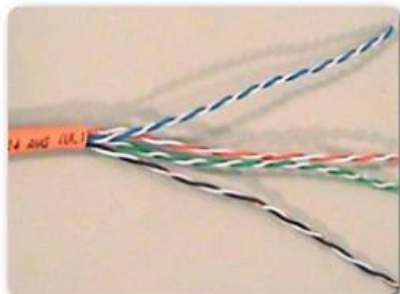
- Layer 2 addressing
 - MAC address (NIC)
 - Communicate on the same network (till gateway)
- Layer 3 addressing
 - IP address
 - Communicate on different network (through gateway)

Chapter 4



Synchroon: gelijke tussentijden voor signalen.

Asynchroon: niet gelijke tussentijden voor signalen.



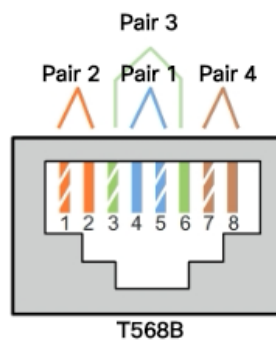
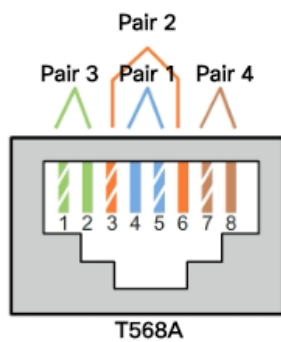
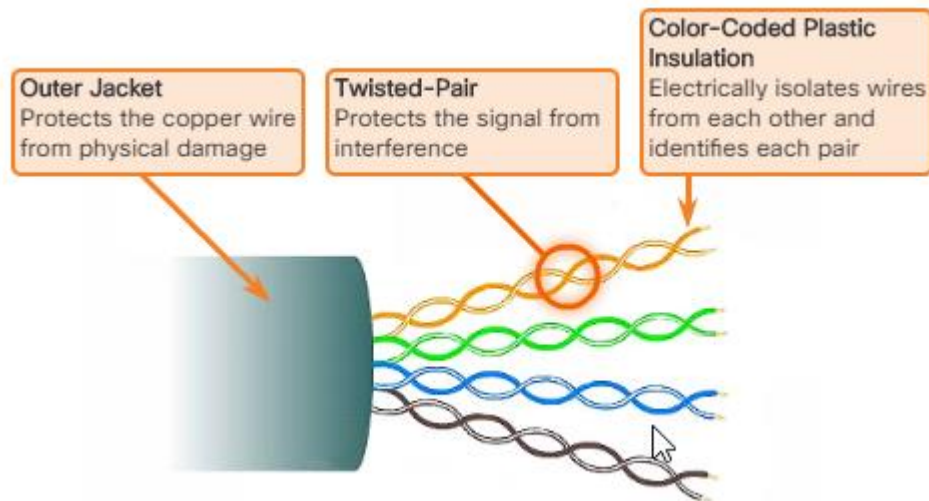
Unshielded Twisted-Pair
(UTP) cable



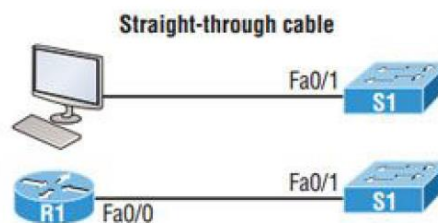
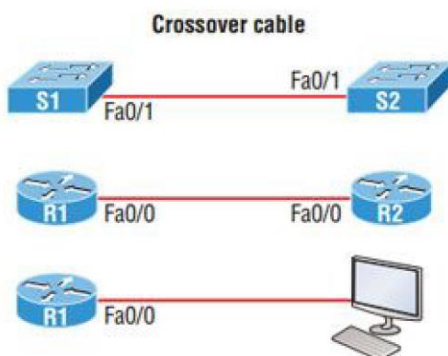
Shielded Twisted-Pair
(STP) cable

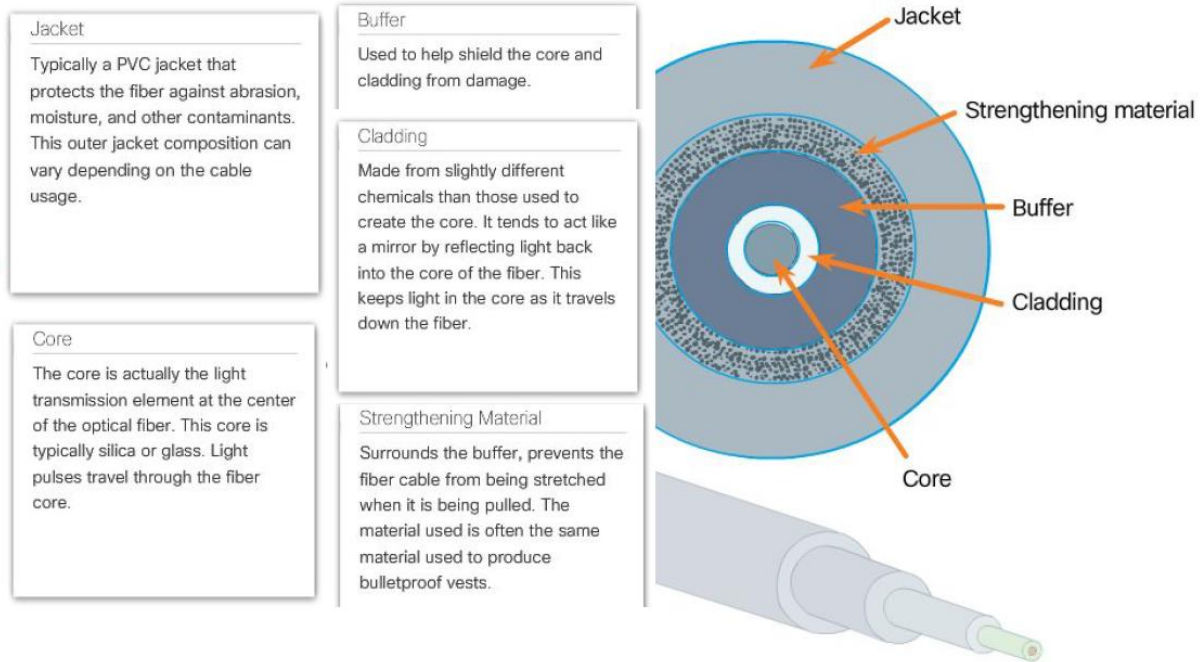


Coaxial cable

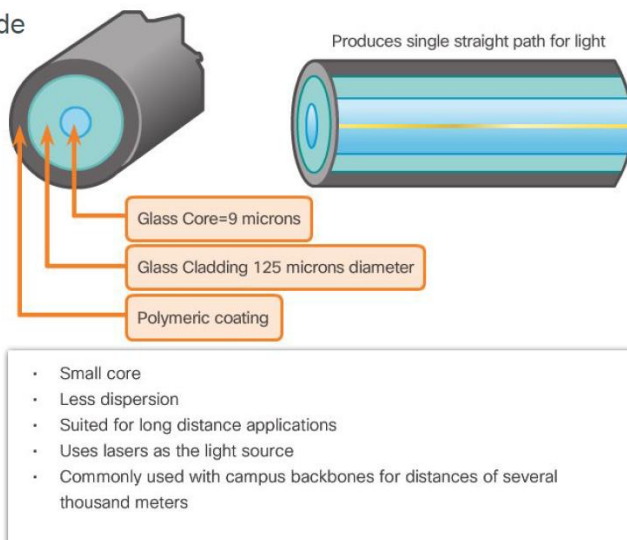


| Cable Type | Standard | Application |
|---------------------------|------------------------------------|---|
| Ethernet Straight-through | Both ends T568A or both ends T568B | Connects a network host to a network device such as a switch or hub. |
| Ethernet Crossover | One end T568A, other end T568B | <ul style="list-style-type: none"> Connects two network hosts Connects two network intermediary devices (switch to switch, or router to router) |
| Rollover | Cisco proprietary | Connects a workstation serial port to a router console port, using an adapter. |

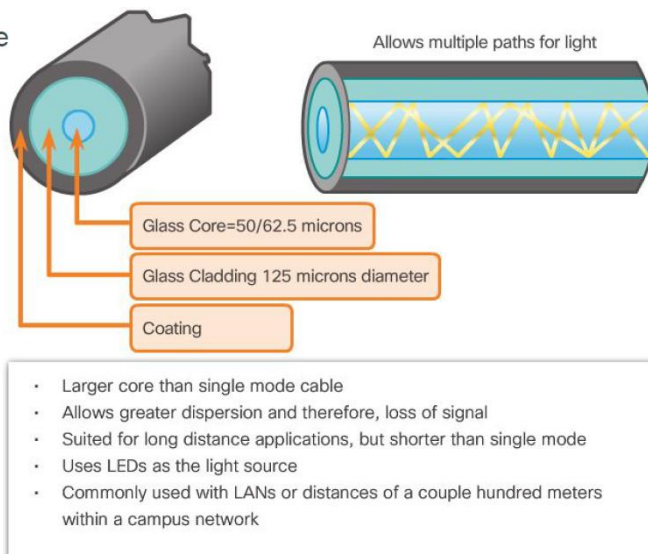




Single Mode



Multimode



Common Fiber Patch Cords



SC-SC Multimode Patch Cord



LC-LC Single-mode Patch Cord



ST-LC Multimode Patch Cord



SC-ST Single-mode Patch Cord

Optical Time Domain Reflectometer (OTDR)

Three common types of fiber-optic termination and splicing errors are:

- **Misalignment:** The fiber-optic media are not precisely aligned to one another when joined.
- **End gap:** The media does not completely touch at the splice or connection.
- **End finish:** The media ends are not well polished, or dirt is present at the termination.

Wi-Fi: Standard IEEE
802.11

Standard IEEE 802.15:
Bluetooth:

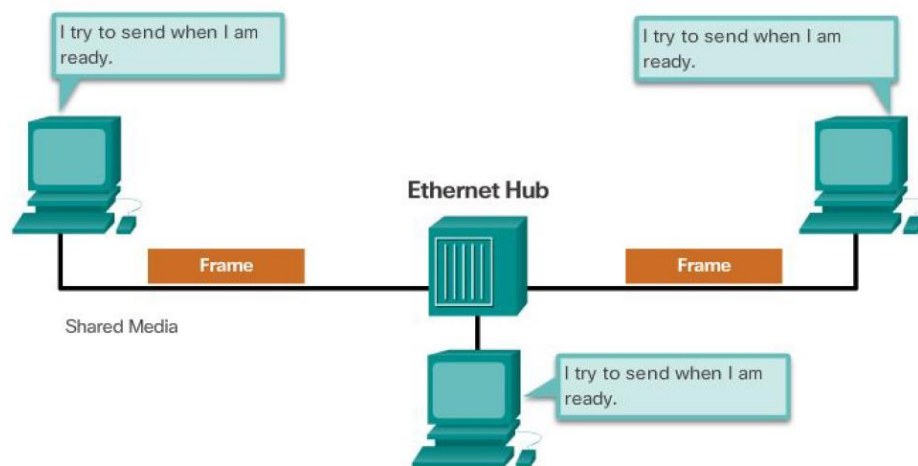
Standard IEEE 802.16:
WiMAX:

Commonly known as Worldwide Interoperability for Microwave Access (WiMAX), uses a point-to-multipoint topology to provide wireless broadband access.

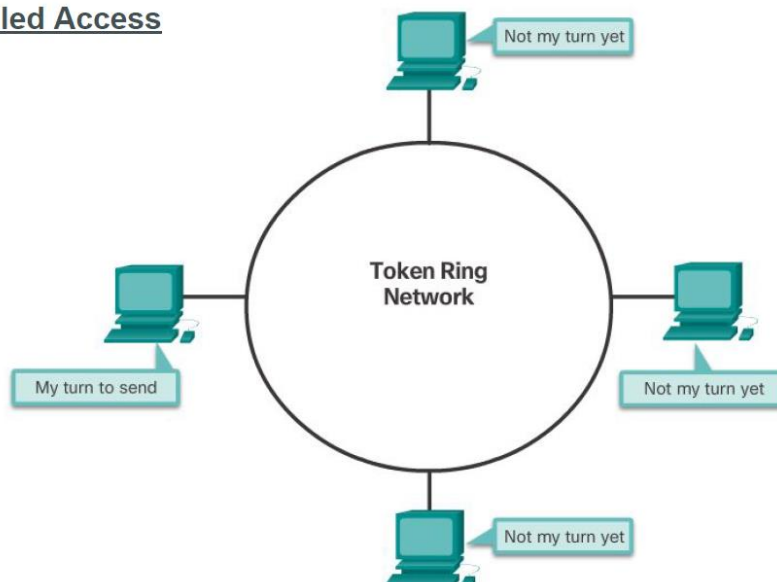
The data link layer is divided into two sublayers:

- **Logical Link Control (LLC)** - This upper sublayer communicates with the network layer. It places information in the frame that identifies which network layer protocol is being used for the frame. This information allows multiple Layer 3 protocols, such as IPv4 and IPv6, to utilize the same network interface and media.
- **Media Access Control (MAC)** - This lower sublayer defines the media access processes performed by the hardware. It provides data link layer addressing and access to various network technologies.

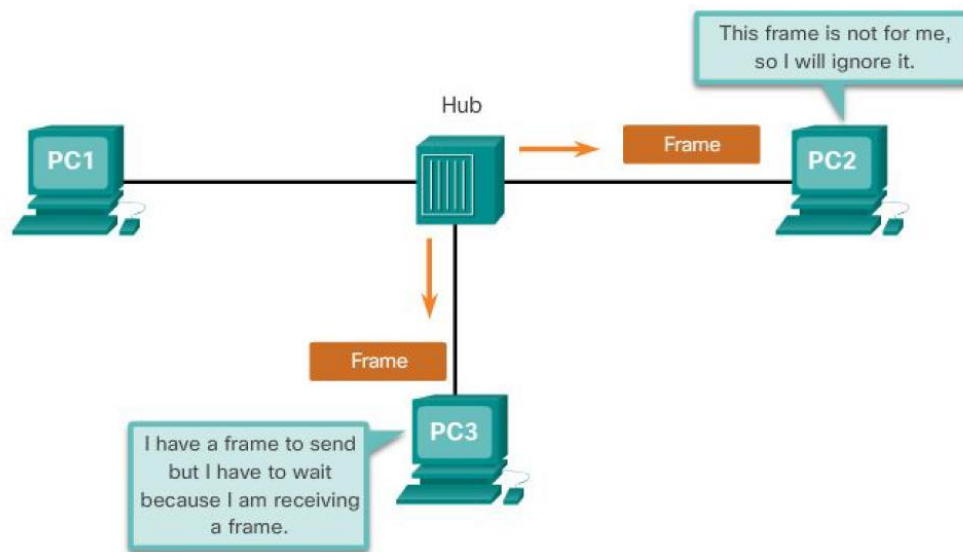
Contention-Based Access



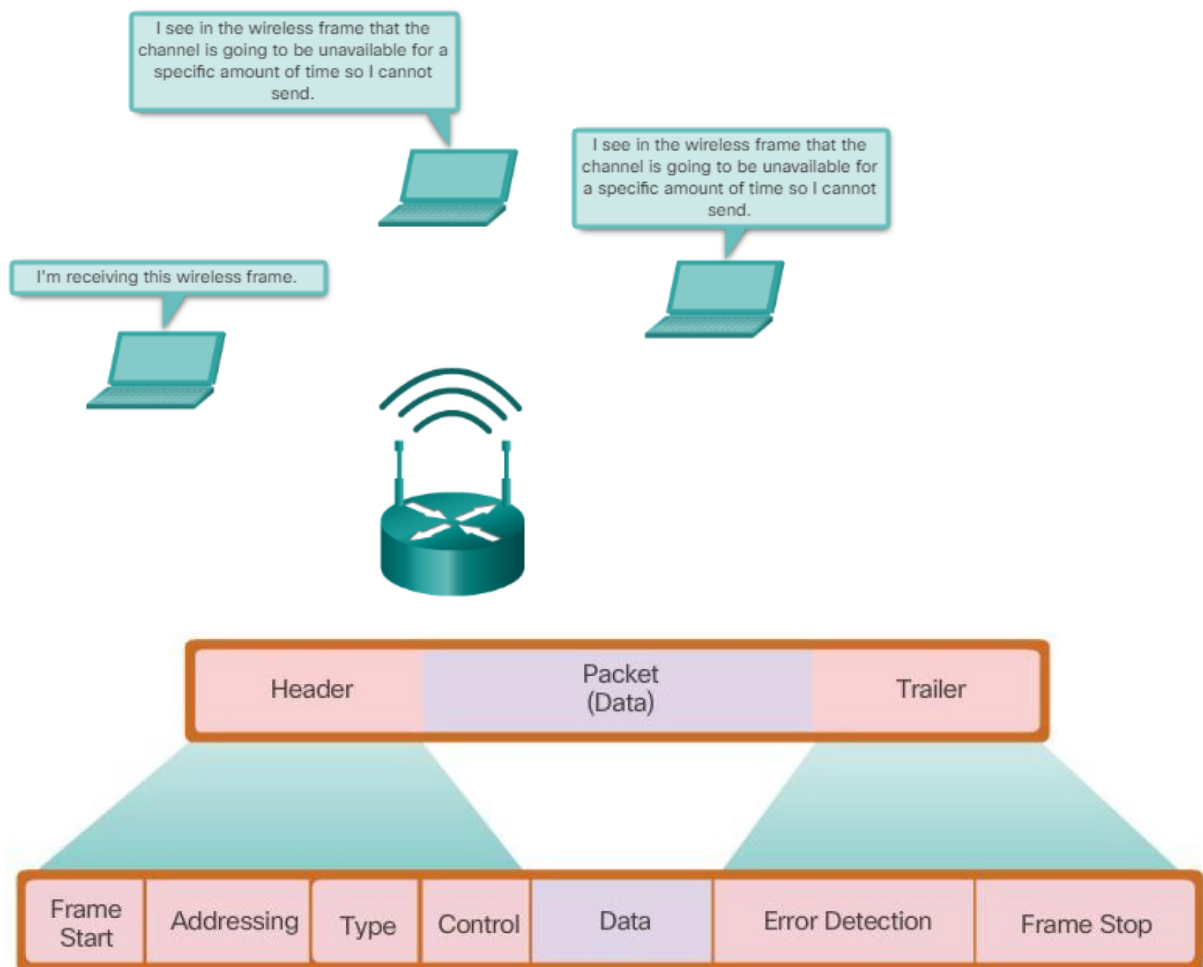
Controlled Access

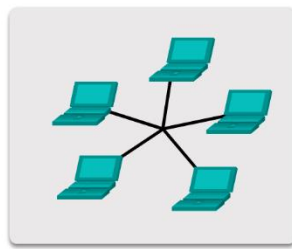


CSMA/CD

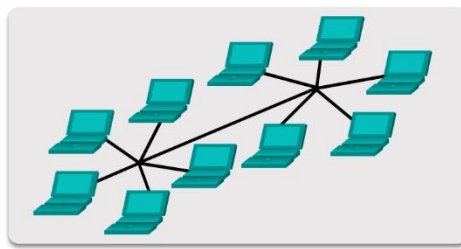


CSMA/CA

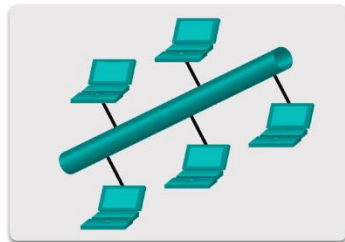




Star topology



Extended star topology



Bus topology



Ring topology

Chapter 5

Ethernet II Frame Structure and Field Size

| Ethernet II | | | | | |
|-------------|---------------------|----------------|---------|------------------|----------------------|
| 8 Bytes | 6 Bytes | 6 Bytes | 2 Bytes | 46 to 1500 Bytes | 4 Bytes |
| Preamble | Destination Address | Source Address | Type | Data | Frame Check Sequence |

MAC Adres:

IEEE requires a vendor to follow two simple rules:

Must use that vendor's assigned OUI as the first three bytes.

All MAC addresses with the same OUI must be assigned a unique value in the last three bytes.

Broadcast: FF-FF-FF-FF-FF-FF of xxx.xxx.xxx.255

Multicast: 224.0.0.0 – 239.255.255.255

Store-and-forward



A store-and-forward switch receives the entire frame, and computes the CRC. If the CRC is valid, the switch looks up the destination address, which determines the outgoing interface. The frame is then forwarded out the correct port.

Cut-through



A cut-through switch forwards the frame before it is entirely received. At a minimum, the destination address of the frame must be read before the frame can be forwarded.

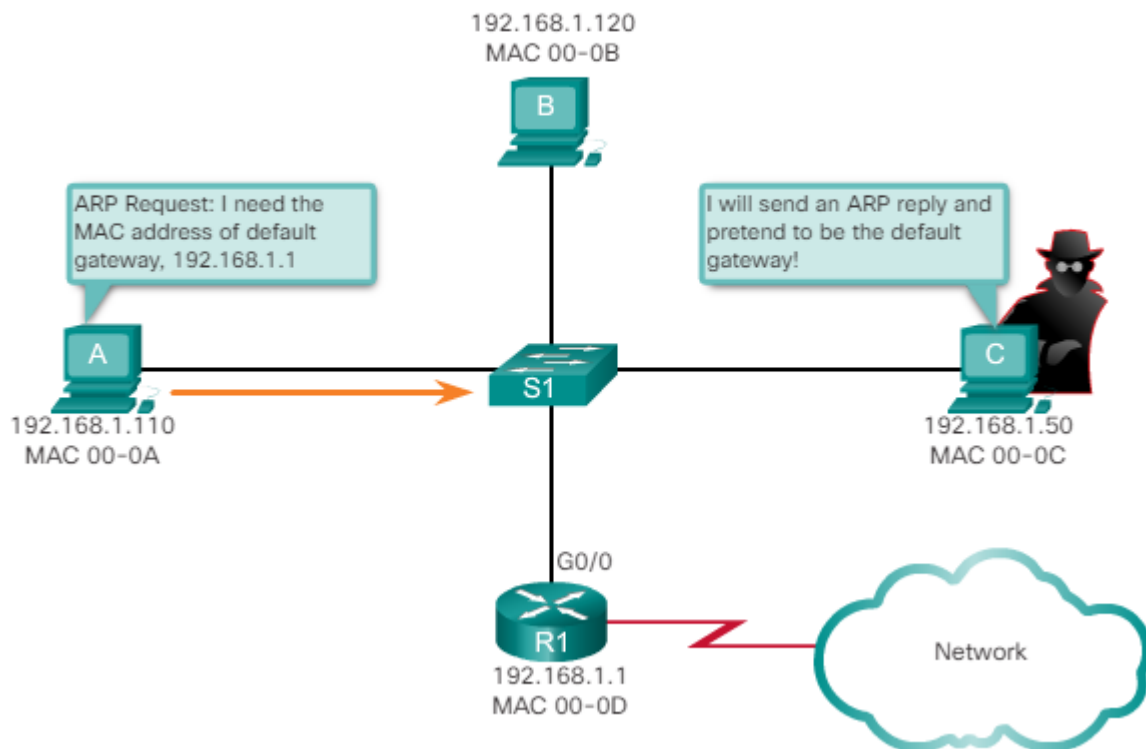
| | |
|-------------------|--|
| Port-based memory | In port-based memory buffering, frames are stored in queues that are linked to specific incoming and outgoing ports. |
| Shared memory | Shared memory buffering deposits all frames into a common memory buffer, which all the ports on the switch share. |

ARP Spoofing

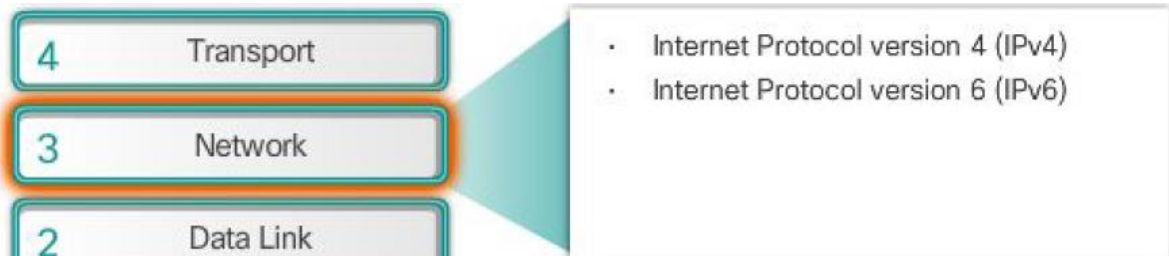
In some cases, the use of ARP can lead to a potential security risk known as ARP spoofing or ARP poisoning. This is a technique used by an attacker to reply to an ARP request for an IPv4 address belonging to another device, such as the default gateway, as shown in the figure. The attacker sends an ARP reply with its own MAC address. The receiver of the ARP reply will add the wrong MAC address to its ARP table and send these packets to the attacker.

- Memory Buffering
 - Port-based memory
 - Frames worden in een wachtrij geplaatst, deze wachtrij is gelinkt aan de uitgaande poorten
 - Shared memory
 - Stopt alle frames in een memory buffer, alle poorten gebruiken deze buffer
- Layer 3 switching
 - Gebruikt ook IP adressen om te switchen (layer 2 enkel MAC)
 - Express forwarding
 - CES = Cisco Express Forwarding
 - Zorgt voor snellere switching integenstelling tot normale layer 3 switches
 - Zorgt ervoor dat er niet constant tussen Layer 2 en 3 wordt gekeken
 - Verschillende interfaces
 - SVI = Switch Virtual Interface = connectie met VLAN
 - Routed Port = Fysieke poort die zich gedraait als een Router poort
 - EtherChannel = Fysieke poort die gelinkt is met een groep van poorten

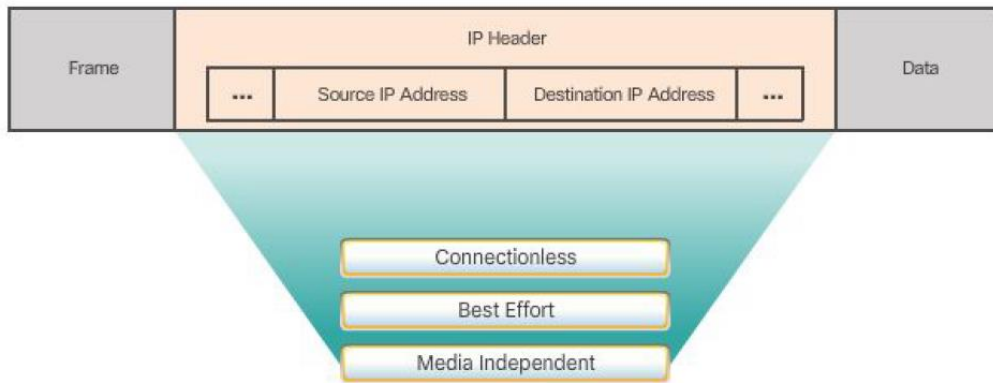
All Devices Powered On at the Same Time



Chapter 6



6.1.2.2 Characteristics of IP



Connectionless

No connection with the destination is established before sending data packets.

Best Effort

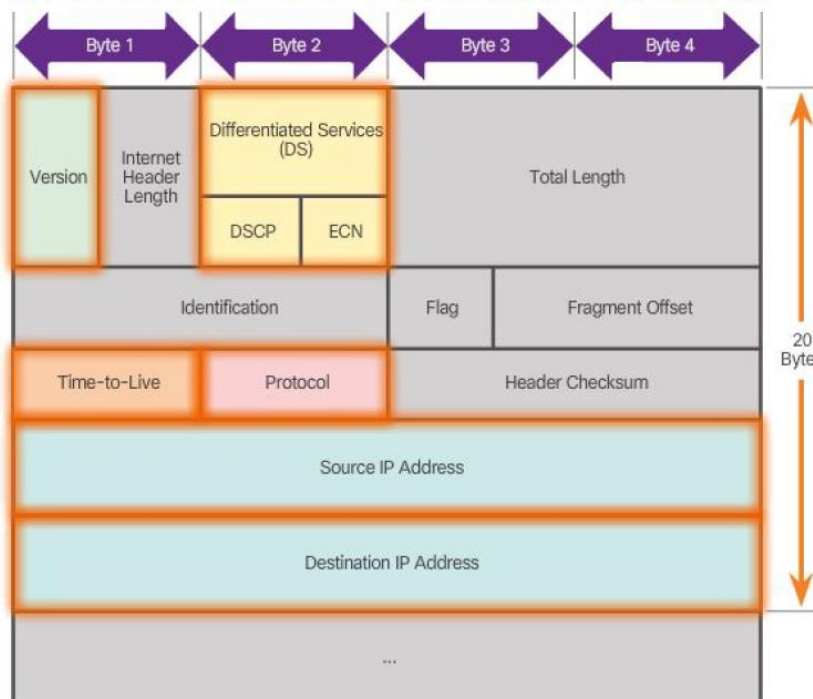
IP is inherently unreliable because packet delivery is not guaranteed.

Media Independent

Operation is independent of the medium (i.e., copper, fiber optic, or wireless) carrying the data.

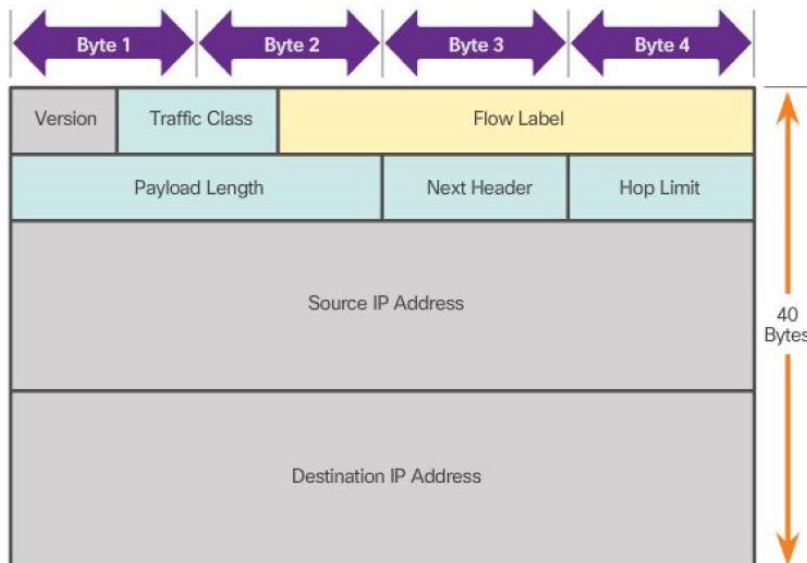
Cisco Public 14

6.1.3.1 IPv4 Packet Header



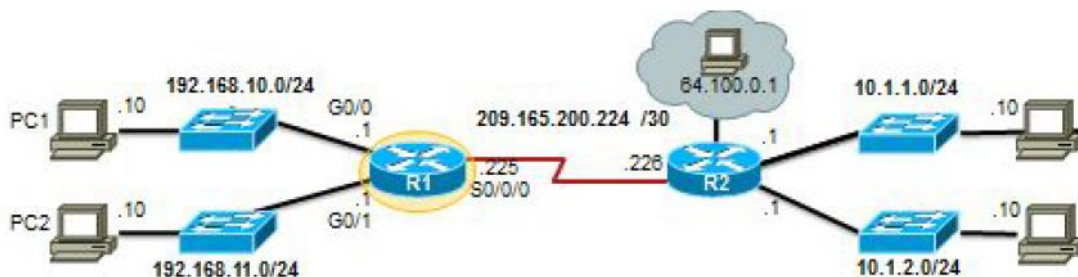
IPv6 Packet Header

Fields in the IPv6 Packet Header



Verbeteringen door IPv6

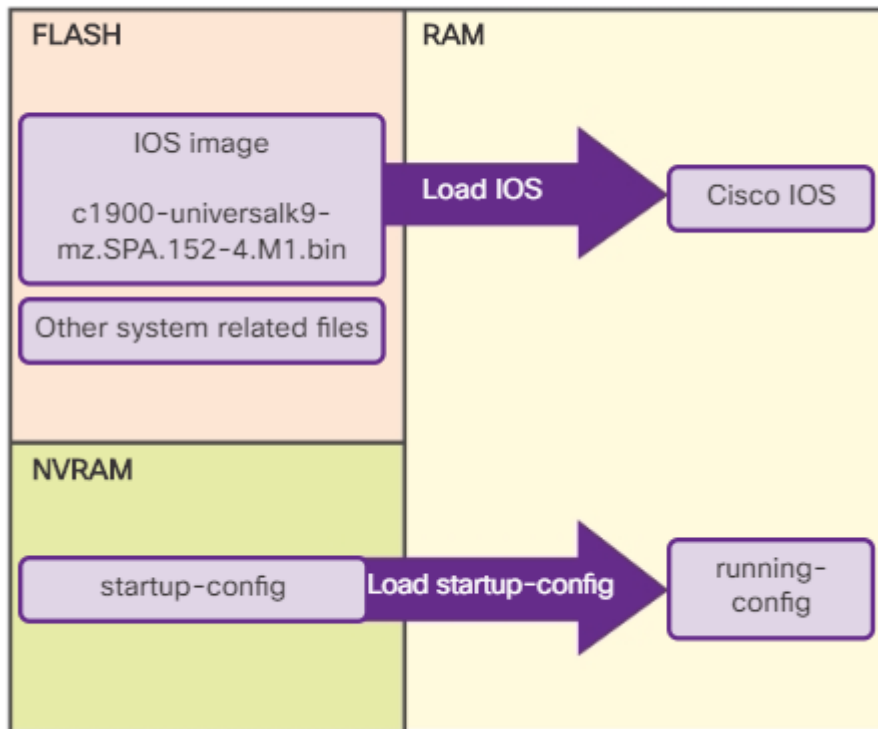
- Meer adresruimte (128-bit tov 32-bit)
- Betere packet behandeling (minder velden)
- Geen NAT meer nodig (gezinnen tot bedrijven kunnen hun persoonlijk publiek IPv6 adres verkrijgen)
- Geïntegreerde beveiliging (authentication)



| | | | | | | |
|---|-------------|--------------|-----|-----------------|----------|-------------|
| D | 10.1.1.0/24 | [90/2170112] | via | 209.165.200.226 | 00:00:05 | Serial0/0/0 |
|---|-------------|--------------|-----|-----------------|----------|-------------|

| | |
|---|---|
| A | Identifies how the network was learned by the router. |
| B | Identifies the destination network. |
| C | Identifies the administrative distance (trustworthiness) of the route source. |
| D | Identifies the metric to reach the remote network. |
| E | Identifies the next hop IP address to reach the remote network. |
| F | Identifies the amount of elapsed time since the network was discovered. |
| G | Identifies the outgoing interface on the router to reach the destination network. |

Files Copied to RAM During Bootup

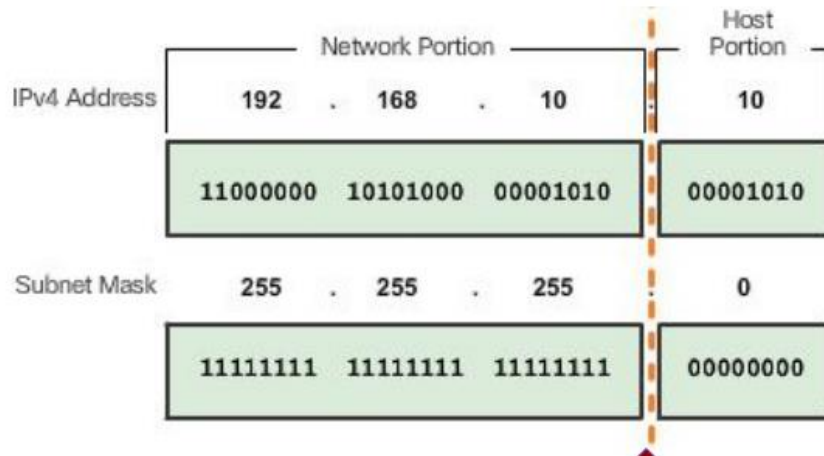


Memory

- **RAM**
 - Cisco IOS wordt gekopieerd naar de RAM bij de bootup
 - Running configuration file
 - IP routing table
 - ARP cache
 - Packet buffer
- **ROM**
 - Bootup instruction
 - Diagnostic software
 - Limited IOS (backup)
- **NVRAM**
 - Permanente opslag
 - Startup-configuration
- **Flash**
 - Permanente opslag
 - IOS wordt van hier uit gekopieerd naar het RAM geheugen bij bootup

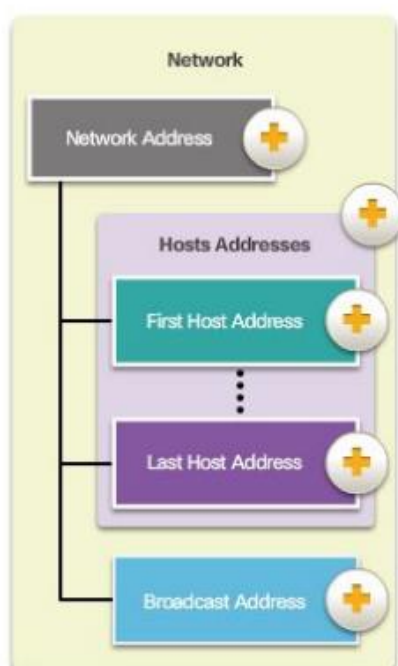
Chapter 7

One portion of the 32 bit IPv4 address identifies the network, and another portion identifies the host.



| Subnet Mask | 32-bit Address | Prefix Length |
|-----------------|-------------------------------------|---------------|
| 255.0.0.0 | 11111111.00000000.00000000.00000000 | /8 |
| 255.255.0.0 | 11111111.11111111.00000000.00000000 | /16 |
| 255.255.255.0 | 11111111.11111111.11111111.00000000 | /24 |
| 255.255.255.128 | 11111111.11111111.11111111.10000000 | /25 |
| 255.255.255.192 | 11111111.11111111.11111111.11000000 | /26 |
| 255.255.255.224 | 11111111.11111111.11111111.11100000 | /27 |
| 255.255.255.240 | 11111111.11111111.11111111.11110000 | /28 |
| 255.255.255.248 | 11111111.11111111.11111111.11111000 | /29 |
| 255.255.255.252 | 11111111.11111111.11111111.11111100 | /30 |

Getal achter de / zegt hoeveel 1'en er gebruikt worden!



The 224.0.0.0 to 239.255.255.255 range of addresses are reserved for multicast.

Source: 172.16.4.1

Private Addresses:

- 10.0.0.0/8 or 10.0.0.0 to 10.255.255.255
- 172.16.0.0 /12 or 172.16.0.0 to 172.31.255.255
- 192.168.0.0 /16 or 192.168.0.0 to 192.168.255.255

7.1.4.3 Special Use IPv4 Addresses

- Loopback addresses
127.0.0.0 /8 or 127.0.0.1 to 127.255.255.254
- Link-Local addresses or Automatic Private IP Addressing (APIPA) addresses
169.254.0.0 /16 or
169.254.0.1 to 169.254.255.254
- TEST-NET addresses
192.0.2.0/24 or 192.0.2.1
to 192.0.2.254

Pinging the Loopback Interface

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\NetAcad> ping 127.0.0.1

Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time=0ms TTL=128
Reply from 127.0.0.1: bytes=32 time=0ms TTL=128
Reply from 127.0.0.1: bytes=32 time=0ms TTL=128
Reply from 127.0.0.1: bytes=32 time=0ms TTL=128
```

IPV6

- **Dual-stack:** allows IPv4 and IPv6 to coexist on the same network. Devices run both IPv4 and IPv6 protocol stacks simultaneously.
- **Tunneling:** is a method of transporting an IPv6 packet over an IPv4 network. The IPv6 packet is encapsulated inside an IPv4 packet.
- **Translation:** Network Address Translation 64 (NAT64) allows IPv6-enabled devices to communicate with IPv4-enabled devices using a translation technique similar to NAT for IPv4. An IPv6 packet is translated to an IPv4 packet, and vice versa.

Tunnelling

FFFF = hextet

F = nibble

- Een combinatie van source en destination IP-adressen en poortnummers worden **Sockets** genoemd
 - Verzender: 192.168.1.5:1099 (host-computer)
 - Ontvanger: 192.168.1.7:80 (web-server)
 - Samen vormen deze een **socket-pair**
 - 192.168.1.5:1099, 192.168.1.7:80

7.2.2.2 Rule 1 – Omit Leading 0's

Example 1

| | |
|---------------|---|
| Preferred | 2001:0DB8:0000:1111:0000:0000:0000:0200 |
| No leading 0s | 2001: DB8: 0:1111: 0: 0: 0: 200 |

7.2.2.3 Rule 2 – Omit All 0 Segments

Example 1

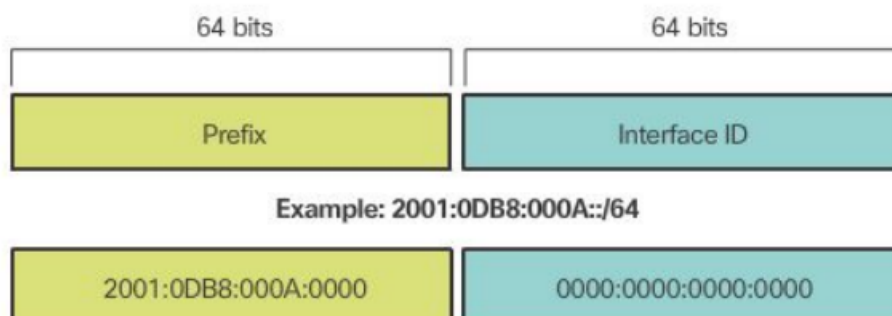
| | |
|---------------|---|
| Preferred | 2001:0DB8:0000:1111:0000:0000:0000:0200 |
| No leading 0s | 2001: DB8: 0:1111: 0: 0: 0: 200 |
| Compressed | 2001:DB8:0:1111::200 |

Er mag maar 1 :: gebruikt worden!

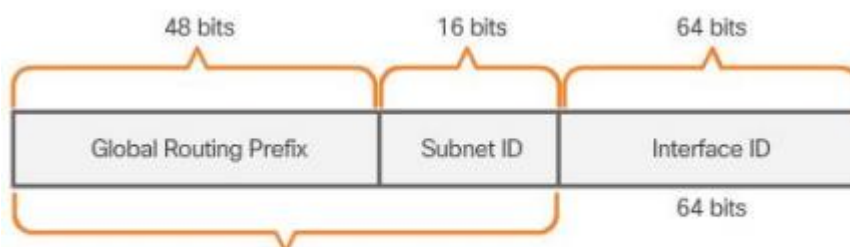
Note: IPv6 does not have broadcast addresses.

7.2.3.2 IPv6 Prefix Length

- IPv6 does not use the dotted-decimal subnet mask notation.
- Prefix length indicates the network portion of an IPv6 address using the following format:
 - IPv6 address /prefix length
 - Prefix length can range from 0 to 128
 - Typical prefix length is /64



| | |
|-------------------------------------|--|
| Global Unicast 2001:db8/64 | Public addresses |
| Link-local FE80::1 | 169.254 (APIPA) |
| Loopback ::1/128 | 127.0.0.1 |
| Unspecified Address ::/128 | enkel als source als host nog geen IP |
| Unique Local FC00::/7 - FDFF::/7 | Private addresses |
| Embedded IPv4 | IPv6 with embedded IPv4 |



A /48 routing prefix + 16 bit Subnet ID = /64 prefix.

Router Advertisement Options

Option 1 (SLAAC Only) - "I'm everything you need (Prefix, Prefix-length, Default Gateway)"

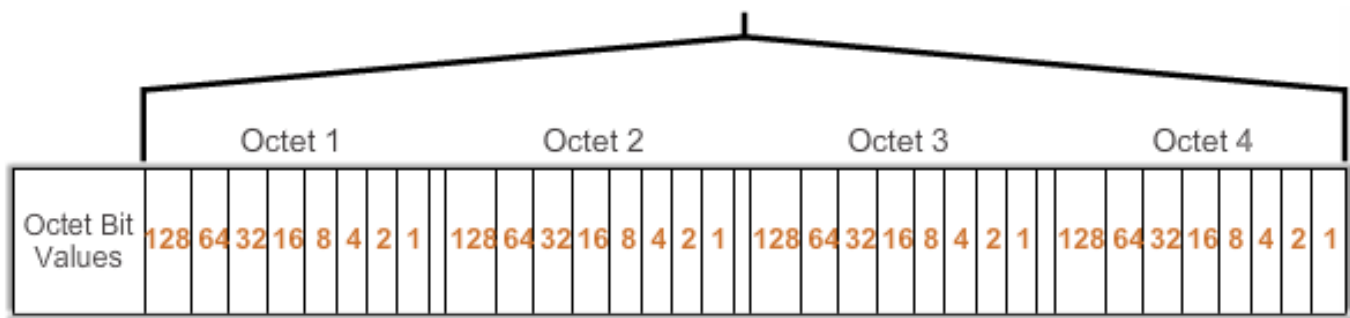
Option 2 (SLAAC and DHCPv6) - "Here is my information but you need to get other information such as DNS addresses from a DHCPv6 server."

Option 3 (DHCPv6 Only) - "I can't help you. Ask a DHCPv6 server for all your

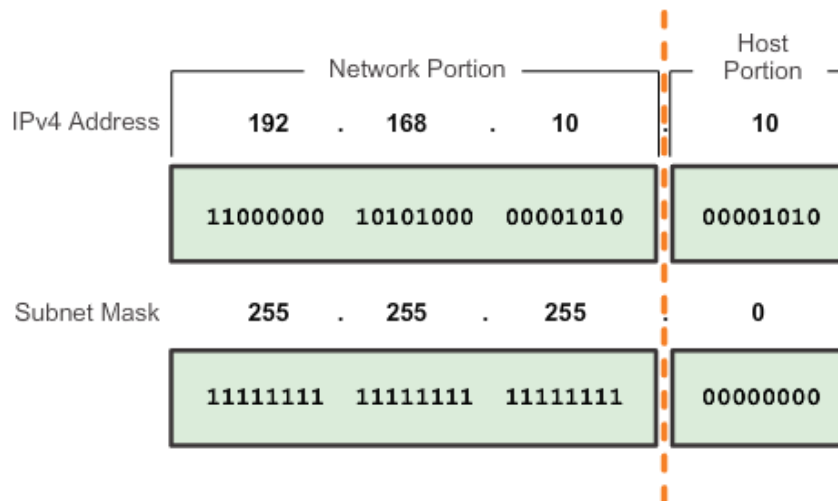
- ICMP messages common to both ICMPv4 and ICMPv6 include:
 - Host confirmation
 - Destination or service unreachable
 - Time exceeded
 - Route redirection
- Although IP is not a reliable protocol, the TCP/IP suite provides for messages to be sent in the event of certain errors. They are sent using the services of ICMP.

Chapter 8

- IPv4 adressen zijn 32-bit binaire nummers
- Voor gebruik door mensen worden deze decimaal uitgedrukt
- Een IP-adres is een hiërarchisch adres dat bestaat uit een Netwerk-deel en Host-deel
- Om te zien welk deel wat is, moet het 32-bit getal bekeken worden
- Het netwerk-deel is identiek voor alle hosts in hetzelfde netwerk
- Dit binair nummer wordt gesplitst in 4 bytes (octet)
 - 11000000 10101000 00001010 00001010
 - oftewel
 - 192.168.10.10
- Iedere byte kan een maximale waarde van 255 hebben
 - bv: 11111111
- Iedere byte kan een minimale waarde van 0 hebben
 - bv: 00000000



- IPv4 Subnet Masks
 - Wanneer een host een IP krijgt wordt er een subnet mask aan toegekend
 - Dit subnet mask is ook 32-bit lang
 - Dit subnet mask bepaalt welk deel van het IP-adres het netwerk deel en het host deel is



- Het aantal bits dat op 1 staat wordt ook wel de **Prefix** genoemd
- In decimale notatie wordt dit weergegeven in de slash-notatie

| | Dotted Decimal | Significant bits shown in binary |
|---------------------------------------|----------------|----------------------------------|
| Network Address | 10.1.1.0/27 | 10.1.1.00000000 |
| First Host Address | 10.1.1.1 | 10.1.1.00000001 |
| Last Host Address | 10.1.1.30 | 10.1.1.00011110 |
| Broadcast Address | 10.1.1.31 | 10.1.1.00011111 |
| Number of hosts: $2^5 - 2 = 30$ hosts | | |

- Er zijn drie types van adressen in een IPv4 network
 - Network address
 - Dit is de standaard manier om naar een netwerk te refereren
 - Bv het "10.1.1.0" netwerk
 - oftewel
 - Bv het "10.1.1.0 255.255.255" netwerk
 - Alle hosts in het "10.1.1.0/24" netwerk zullen dezelfde netwerk deel bits hebben
 - Host addresses
 - Iedere host heeft een uniek adres
 - Deze adressen liggen tussen het network address en het Broadcast address
 - Deze adressen kunnen dus nooit op 00000000 of 11111111 eindigen
 - Broadcast address
 - Dit is een speciaal adres voor ieder netwerk om te communiceren met ALLE hosts op het netwerk
 - Een host kan een packet verzenden via dit adres, vervolgens zullen alle hosts dit packet ontvangen
 - Dit adres gebruikt het hoogste adres in het bereik (alle bits op 1 oftewel 255)
- Het eerste en laatste Host-adres
 - Het eerste Host-adres zal altijd 1 hoger zijn dan het Network-adres
 - In een "10.1.1.0/24" netwerk zal de eerste Host het IP-adres 10.1.1.1 krijgen
 - Het eerste Host-adres is meestal voor de Router of Default Gateway voorzien
 - Het laatste Host-adres zal allemaal 1 bits bevatten, maar een 0 voor de meest rechtse bit
 - In een "10.1.1.0/24" netwerk zal de laatste host het IP-adres 10.1.1.254 krijgen

- Bitwise AND Operation
 - De AND operatie is 1 van de 3 basis operaties die gebruikt worden
 - De andere twee zijn OR en NOT
 - Het IPv4 adres word ge-AND, bit per bit, met het subnet mask om het Netwerk-deel van het IP adres te vormen
 - Dit wordt gebruikt om de host-bits te "maskeren"

- In een IPv4 netwerk kan een host op drie verschillende manieren communiceren
 - Unicast
 - Een packet verzenden van 1 host naar 1 andere host

 - Broadcast
 - Een packet verzenden van 1 host naar alle andere hosts

 - Multicast
 - Een packet verzenden van 1 host naar een specifieke groep van andere hosts

- Network, Broadcast en Host adressen berekenen

- Types van IPv4-adressen
 - De meeste IPv4 host adressen zijn publieke adressen (internetverbinding)
 - Er zijn ook privé-adressen
 - 10.0.0.0 tot 10.255.255.255 (10.0.0.0/8)
 - 172.16.0.0 tot 172.31.255.255 (172.16.0.0/12)
 - 192.168.0.0 tot 192.168.255.255 (192.168.0.0/16)
 - Speciale IP-adressen
 - Loopback 127.0.0.0
 - Verkeer naar zichzelf versturen
 - Link-Local 169.254.0.0 tot 169.254.255.255
 - Adres wanneer er geen IP-adres van de DHCP server verkregen is
 - TEST-NET 192.0.2.0 tot 192.0.2.255
 - Voor documentatie en netwerkvoorbeelden
 - Experimentele adressen 240.0.0.0 tot 255.255.255.254
 - Gereserveerd voor toekomstig gebruik
 - Classful addressing
 - Werd in het verleden gebruikt
 - Class A Blocks
 - Extreem grote netwerken (meer dan 16.000.000 hosts)
 - Class B Blocks
 - Gemiddeld grote netwerken (meer dan 65000 hosts)
 - Class C Blocks
 - Kleine netwerken (maximaal 254 hosts)
 - Classful addressing was niet erg efficient
 - In 1993 werd er een nieuwe standaard ontwikkeld
 - Classless addressing (CIDR)
 - Publieke IP-adressen toewijzen
 - Deze moeten uniek zijn aangezien ze toegankelijk zijn vanaf het internet
 - Web servers bv

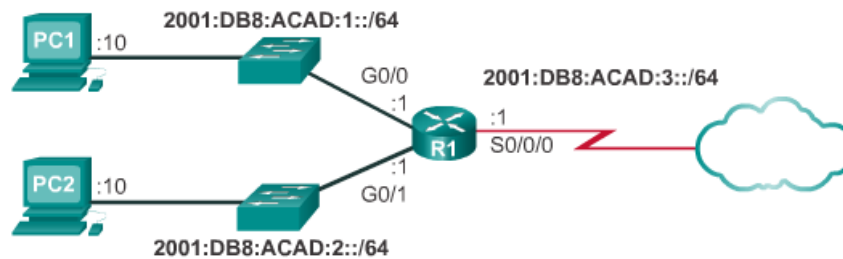
- Deze werden tot mid-1990 beheerd door IANA
- De IP-address-space die er nog over was beheerd door RIRs
 - AfrNIC African Network Information Centre
 - APNIC Asia Pacific Registry for Internet Numbers
 - ARIN American Registry for Internet Numbers
 - LACNIC Latin-American/Caribbean IP Address Registry
 - RIPE NCC Reseaux IP Europeans
- Om een verbinding met het internet te verkrijgen moeten we verbinden met een Internet Service Provider (ISP)
 - Er zijn verschillende niveaus van ISPs
 - Tier 1
 - Top van de Internet ISPs
 - Hoge betrouwbaarheid
 - Hoge kosten
 - Tier 2
 - Deze Tiers krijgen hun verbinding via Tier 1 ISPs
 - Beheren vaak zelf hun eigen DNS, Email en Web servers
 - Bieden vaak ook onderhoud, e-commerce/business en VoIP aan
 - Tier 3
 - Deze Tiers krijgen hun verbinding via Tier 2 ISPs
 - Bieden internet services aan voor thuisgebruik / winkels
 - Hun hoofddoel is connectiviteit en support
 - Bieden vaak gebundelde contracten aan voor hun klanten
 - Zijn vaak iets minder betrouwbaar en hebben een tragere verbinding
 - Maar zijn even vaak een goede keuze voor kleine tot grote bedrijven
- IPv6
 - IPv6 is ontworpen als opvolger van IPv4
 - IPv6 heeft een grotere 128-bit address-space (340 undeciljoen adressen)
 - Er is geen definitieve datum om van IPv4 naar IPv6 over te schakelen
 - De overgang wordt zal waarschijnlijk jaren duren
 - Er zijn protocollen ontworpen om administrators te helpen om hun netwerken te migreren naar IPv6
 - Dual Stack
 - Zorgt ervoor de IPv4 en IPv6 op 1 netwerk kunnen bestaan
 - Apparaten draaien het IPv4 en IPv6 protocol tegelijk
 - Tunneling
 - Zorgt ervoor dat IPv6 packets over een IPv4 netwerk kunnen verstuurd worden via Encapsulation
 - Translation
 - Zorgt ervoor dat IPv6 apparaten met IPv4 apparaten kunnen communiceren via een translation-techniek.
 - IPv4 packets worden vertaald naar IPv6 en omgekeerd.
 - IPv6 adressen worden niet decimaal voorgesteld, maar hexadecimaal
 - In totaal zijn er 32 hexadecimale waarden in een IPv6 adres
 - Elke 4-bits stellen 1 hexadecimaal getal voor
 - Elke 16-bits worden een hextet genoemd
 - "Leading zeroes" worden weg gelaten in een hextet om de notatie te verkorten
 - 01AB -> 1AB
 - 09F0 -> 9F0
 - etc

- 16-bit segmenten die enkel **nullen** bevatten worden vervangen door een double colon "::".
- Via deze 2 technieken kan een IPv6-adres sterk verkort worden

| | |
|---------------|------------------------------------|
| Preferred | FE80:0000:0000:0123:4567:89AB:CDEF |
| No leading 0s | FE80: 0: 0: 0: 123:4567:89AB:CDEF |
| Compressed | FE80::123:4567:89AB:CDEF |

- Er zijn zoals bij IPv4, drie verschillende types van IPv6 adressen
 - Unicast
 - Broadcast
 - Multicast
- Net zoals bij IPv4 is er een **Prefix**
 - Vaak is deze prefix /64
 - De eerste 64-bits zijn dan het netwerkdeel
 - De laatste 64 bits zijn dan het hostdeel
- Types van IPv6 adressen

| | | |
|-----------------------------|---|---------------------------|
| ▪ Global Unicast | = | Public IPv4 adres |
| ▪ Link-Local | = | Lokaal IP-adres |
| ▪ Loopback | = | Communiceren met zichzelf |
| ▪ Unspecified Address | = | Allemaal nullen of /128 |
| ▪ Unique Local | = | Private IPv4 adres |
| ▪ IPv4 Embedded (migration) | = | Bevat een IPv4 adres |
- Iedere IPv6 NIC is **verplicht** om een IPv6 Link-Local adres te hebben
 - Indien er geen is toegewezen, zal het apparaat er zelf eentje instellen
- De meeste IPv6 commandos in de Cisco IOS zijn identiek aan die van de IPv4 commandos
 - Het enige verschil is dat men ipv6 ipv ip moet gebruiken in de commandos



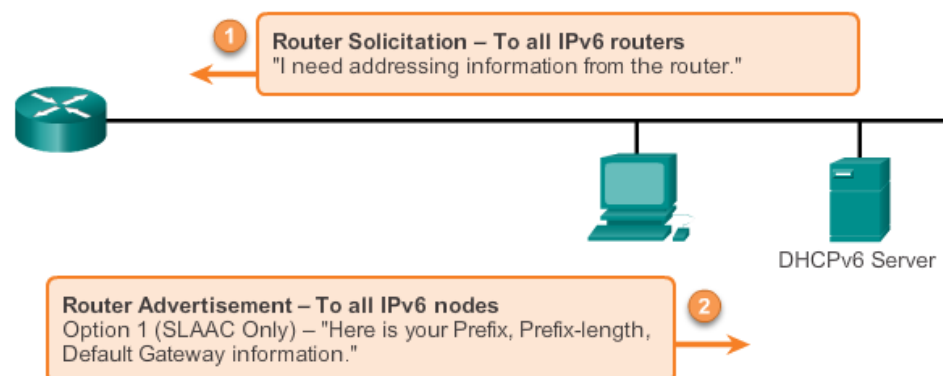
```

R1(config)#interface gigabitethernet 0/0
R1(config-if)#ipv6 address 2001:db8:acad:1::1/64
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface gigabitethernet 0/1
R1(config-if)#ipv6 address 2001:db8:acad:2::1/64
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface serial 0/0/0
R1(config-if)#ipv6 address 2001:db8:acad:3::1/64
R1(config-if)#clock rate 56000
R1(config-if)#no shutdown

```

○ SLAAC

- Stateless Address Autoconfiguration
- Een methode dat een apparaat toestaat zijn prefix, prefix length en default gateway van de Router te verkrijgen zonder het gebruik van een IPv6-server.
- De router zal Router Advertisement Messages (RA) uitzenden
- De apparaten verkrijgen via deze RA de benodigde informatie.



Router Advertisement Options

- Option 1 (SLAAC Only)** – "I'm everything you need (Prefix, Prefix-length, Default Gateway)"
- Option 2 (SLAAC and DHCPv6)** – "Here is my information but you need to get other information such as DNS addresses from a DHCPv6 server."
- Option 3 (DHCPv6 Only)** – "I can't help you. Ask a DHCPv6 server for all your information."

○ DHCPv6

- Vergelijkbaar met DHCP voor IPv4
- Een apparaat verkrijgt zijn Unicast-adres, prefix length, default gateway en DNS-adressen van de DHCPv6-server

- EUI-64 Proces
 - Dit proces gebruikt een host zijn 48-bit MAC-adres om een 64-bit Interface ID aan te maken
 - MAC-adressen bestaan uit twee delen
 - OUI 24-bit/6 hex digits
 - Device Identifier 24-bit/6 hex digits
 - Een EUI-64 Interface ID herkennen



-
-
- Een apparaat kan ook een Random Generated Interface ID gebruiken
 - Windows Vista gebruikt dit
 - XP en oudere Windows versies gebruiken EUI-64
- Deze Interface IDs kunnen gecombineerd worden met een IPv6-prefix om een Unicast of Link-Local adres te vormen
 - Global Unicast (SLAAC) ICMPv6 RA + Interface ID
 - Link-Local FE80::/64 + Interface ID
- IPv6 Link-Local adressen worden voor verschillen doeleinden gebruikt
 - Een host gebruikt het Link-Local adres van de Router als Default Gateway
 - Routers wisselen Routing Messages uit via dit adres
 - Routing Tables van Routers identificeren de Next-Hop via dit adres

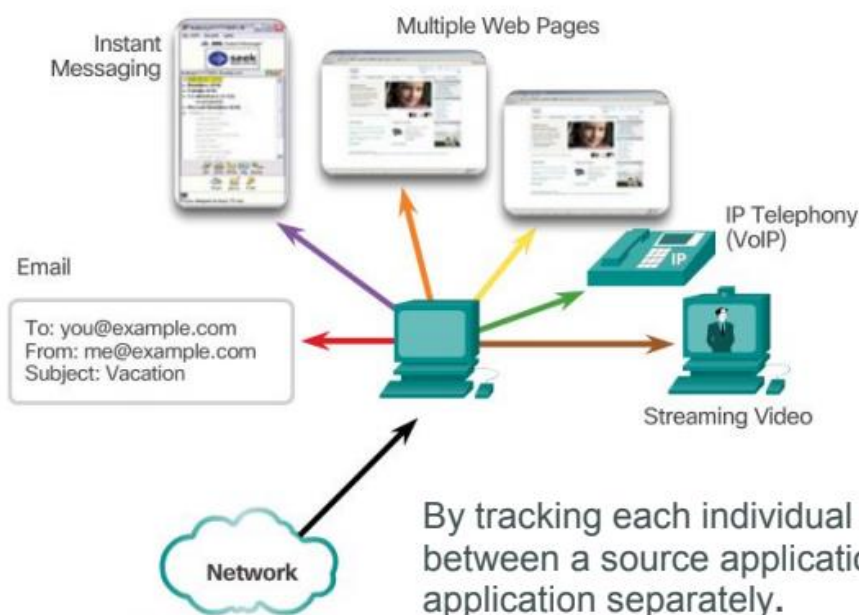
IPv6 Multicast

- Deze zijn vergelijkbaar met IPv4 Multicast adressen (naar meerdere hosts een packet versturen)
- IPv6 Multicast adressen beginnen met FF00::/8
- Er zijn 2 types
 - Assigned Multicast
 - Gereserveerd voor voorgedefinieerde groepen van hosts
 - FF02::1 All-nodes Multicast Group
 - Alle IPv6 apparaten
 - FF02::2 All-routers Multicast Group
 - Alle IPv6 Routers
 - Solicited Node Multicast
 - Vergelijkbaar met All-nodes Multicast Group
 - Enkel de laatste 24-bits van het IPv6 Unicast adres zijn hetzelfde.
 - Enkel die apparaten verwerken de packets
 - Dit adres bestaat uit 2 delen
 - FF02::0:0:0:0:1FF00::/104 prefix
 - Least significant 24-bits
- ICMPv6
 - ICMP is de service die TCP/IP gebruikt om error-messages te versturen
 - ICMPv6 is vergelijkbaar met ICMPv4, maar met extra functionaliteit
 - De messages die beiden ondersteunen zijn
 - Host confirmation
 - Stuurt een Echo Request naar een host om te kijken of deze runt
 - Destination or Service unreachable
 - Gebruiken een numerieke code om de fout te definiëren

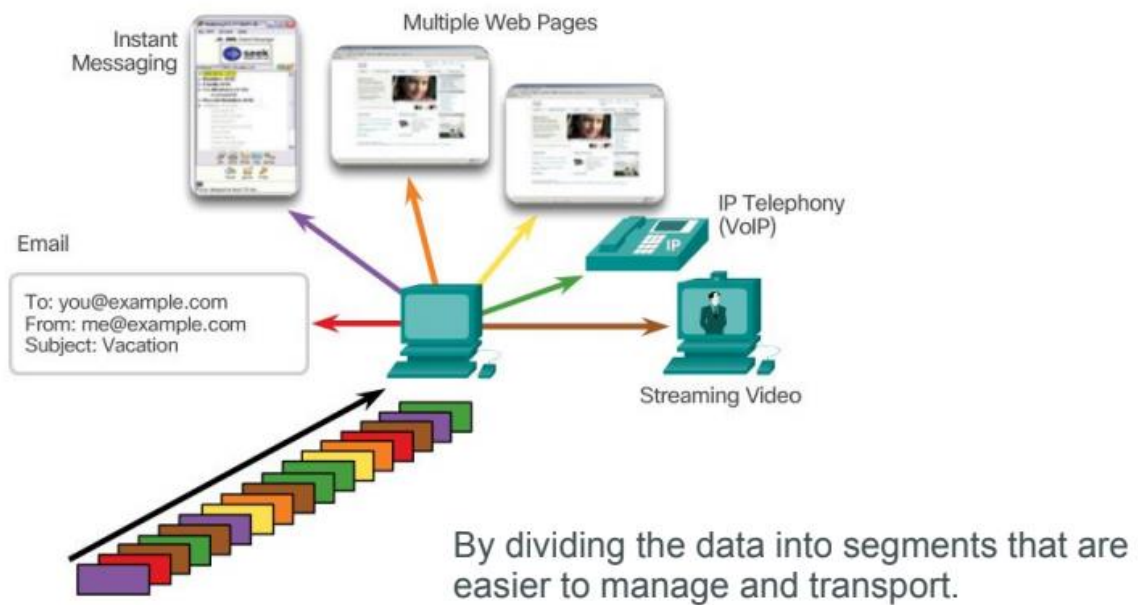
- 0 Net unreachable
 - 1 Host unreachable
 - 2 Protocol unreachable
 - 3 Port unreachable
- Time exceeded
 - Zorgt voor de Timeout error message als het TTL veld op 0 komt bij IPv4
 - IPv6 heeft geen TTL-veld, het gebruikt het Hop-Limit veld
- Route redirection
 - Een router gebruikt deze error-message om een host te verwittigen van een beter pad voor een bepaald destination
- Nieuwe ICMPv6 functionaliteit
 - Router Solicitation Message
 - Router Advertisement Message
 - Neighbor Solicitation Message
 - Neighbor Advertisement Message
- Testing/Verification
 - Ping
 - Ping een andere host test connectie met de andere host
 - Ping local loopback test of TCP/IP runt op de local host
 - Ping Gateway test of de LAN-verbinding actief is
 - Ping remote internetwork test of de verbinding met een actief is
 - Traceroute
 - RTT Round-Trip-Time voor iedere Hop
 - IPv4 TTL
 - IPv6 Hop Limit

Chapter 9

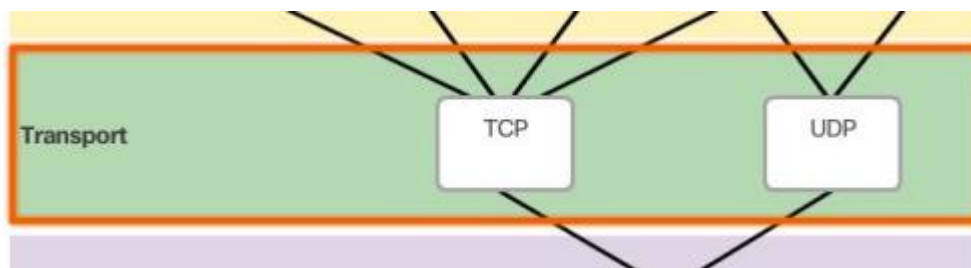
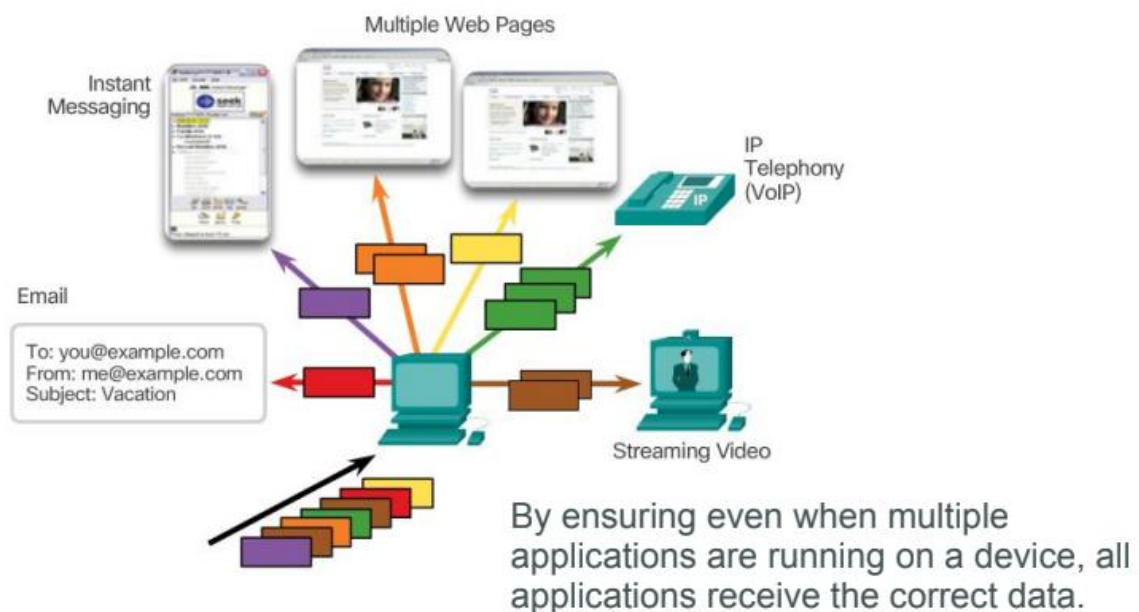
Track Individual Conversations



Segment Data and Reassemble Segments



Identify the Applications



9.1.1.5 TCP

- Reliable (supports packet delivery confirmation)
- 3 basic operations (reliability):
 - Numbering and tracking data segments transmitted
 - Acknowledging received data
 - Retransmitting any unacknowledged data

9.1.1.6 UDP

- reliability is not required
- UDP provides the **basic functions** for delivering data segments between the appropriate applications, with very **little overhead** and data checking.
- Some applications do not require reliability. Reliability incurs additional overhead and possible delays in transmission.
- Adding overhead to ensure reliability for some applications could reduce the usefulness of the application and can even be detrimental.

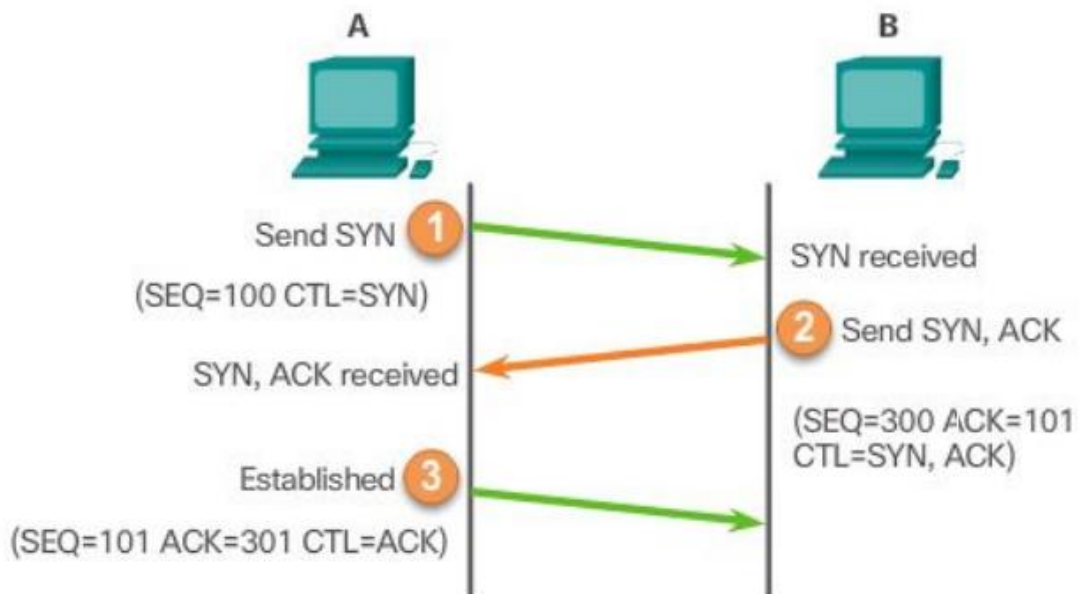
9.1.2.6 Port Numbers

- Source Port is dynamically chosen by the sending device (identify a conversation)
- Destination Port is used to identify an application or service running in the server.

| Port Number | Protocol | Application | Acronym |
|-------------|----------|-------------------------------------|---------|
| 20 | TCP | File Transfer Protocol (data) | FTP |
| 21 | TCP | File Transfer Protocol (control) | FTP |
| 22 | TCP | Secure Shell | SSH |
| 23 | TCP | Telnet | – |
| 25 | TCP | Simple Mail Transfer Protocol | SMTP |
| 53 | UDP, TCP | Domain Name Service | DNS |
| 67, 68 | UDP | Dynamic Host Configuration Protocol | DHCP |
| 69 | UDP | Trivial File Transfer Protocol | TFTP |
| 80 | TCP | Hypertext Transfer Protocol | HTTP |
| 110 | TCP | Post Office Protocol version 3 | POP3 |
| 143 | TCP | Internet Message Access Protocol | IMAP |
| 161 | UDP | Simple Network Management Protocol | SNMP |
| 443 | TCP | Hypertext Transfer Protocol Secure | HTTPS |

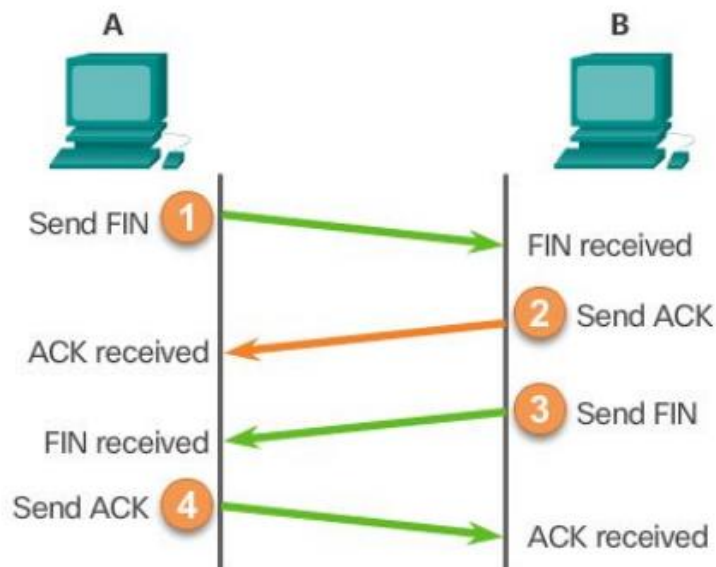
9.2.1.2 TCP Connection Establishment

A TCP connection is established in three steps:



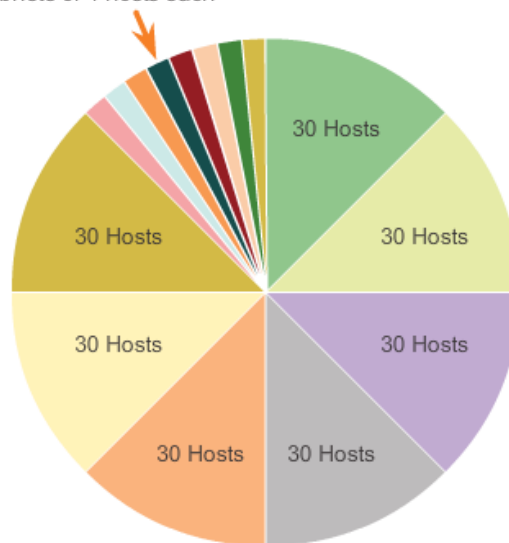
9.2.1.3 TCP Session Termination

The FIN TCP flag is used to terminate a TCP connection.



- VLSM
 - **Variable Length Subnet Masking**
 - Traditionele subnetting gebruikt hetzelfde aantal adressen voor ieder subnet
 - In de realiteit heeft niet ieder subnet evenveel adressen nodig
 - Om het aantal subnetten en adressen te maximaliseren gebruik je dus VLSM
 - Voorbeeld

One subnet was further divided to create 8 smaller subnets of 4 hosts each



○

| | | | |
|-------------------------------------|-------------------------------------|-------------------|--------------------|
| 7 | 11000000.10101000.00010100.11100000 | 192.168.20.224/27 | |
| 3 more bits borrowed from subnet 7: | | | |
| 7:0 | 11000000.10101000.00010100.11100000 | 192.168.20.224/30 | WANs |
| 7:1 | 11000000.10101000.00010100.11100100 | 192.168.20.228/30 | |
| 7:2 | 11000000.10101000.00010100.11101000 | 192.168.20.232/30 | |
| 7:3 | 11000000.10101000.00010100.11101100 | 192.168.20.236/30 | |
| 7:4 | 11000000.10101000.00010100.11110000 | 192.168.20.240/30 | Unused / Available |
| 7:5 | 11000000.10101000.00010100.11110100 | 192.168.20.244/30 | |
| 7:6 | 11000000.10101000.00010100.11111000 | 192.168.20.248/30 | |
| 7:7 | 11000000.10101000.00010100.11111100 | 192.168.20.252/3 | |

Subnetting a subnet

-
- 8 subnetten => 0 - 7
- Het 7de subnet wordt opnieuw in 8 subnetten verdeeld
- $8 \text{ subnetten} = 2^3$
- Je moet dus 3 bits lenen van het 7de subnet

- Basic Subnetting Voorbeeld

| 192.168.5.0/24 Table 1 - First Subnets Calculation | |
|---|-------------------------------|
| Calculate 50 users per subnet | |
| New Subnet Mask (decimal) | 255.255.255.192 ✓ |
| First Prefix notation | /26 ✓ |
| First full subnet range | 192.168.5.0-192.168.5.63 ✓ |
| Second full subnet range | 192.168.5.64-192.168.5.127 ✓ |
| Last full subnet range | 192.168.5.192-192.168.5.255 ✓ |

- 50 users => veelvoud van 2 => 64
- 64 => 6-bits => 32-6=26
- De prefix notatie is dus **/26**
- Het eerste subnet loopt dus van **0 tot en met 63**
- Het tweede subnet loopt van **64 tot en met 127** (64+64=128)
- 128+64=192
- Het laatste subnet loopt van **192 tot en met 255**

- VSLM Subnetting Voorbeeld

| 192.168.5.0/24 Table 2 - VLSM Calculation | |
|---|------------------------------|
| Use Table 1's second full subnet range and VLSM to calculate for 20 users per subnet. | |
| Second full subnet range (/26) from Table 1 | 192.168.5.64-192.168.5.127 ✓ |
| New VLSM Subnet Mask (decimal) | 255.255.255.224 ✓ |
| VLSM Prefix notation | /27 ✓ |
| First full VLSM subnet range | 192.168.5.64-192.168.5.95 ✓ |
| Last full VLSM subnet range | 192.168.5.96-192.168.5.127 ✓ |

- 20 users => veelvoud van 2 => 32
- 32-bits => 5-bits nodig => 32-5=27
- De prefix notatie is dus **/27**
- 64+32=96
- Het eerste VSLM subnet loopt dus van **64 tot en met 95**
- Het tweede VLSM subnet loopt dus van **96 tot en met 127**

- Addressing Schemes
 - Er zijn drie grote factoren om adress allocation te plannen
 - Dubbele adressen voorkomen
 - Toegang tot adressen controleren (servers bv)
 - Performance en Security in de gaten houden (adressen die bv teveel packets versturen of ontvangen)
 - Adressen toewijzen aan Clients
 - User apparaten hebben vaak een dynamisch IP (DHCP)
 - Servers/Printers hebben vaak een statisch IP
 - Enkele apparaten hebben IP-adressen nodig die rechtstreeks toegankelijk zijn vanaf het internet (Servers bv).
 - Hubs/Switches/AP's zijn Intermediary apparaten en krijgen een Layer 3 address om deze te kunnen beheren vanaf het netwerk.
 - Deze apparaten hebben dus ook vaak een statisch IP-adres (voorspelbaarheid)
 - Gateway-apparaten (Routers/Firewalls) hebben een IP-adres ingesteld op iedere interface.
 - Iedere interface zit op een apart netwerk
 - Deze apparaten worden gegroepeerd in logical addressing groups om packet filtering meer efficiënt te maken
 - Deze apparaten hebben een belangrijke security functie
- Subnetting for IPv6
 - Voor IPv6 moet subnetting op een andere manier aangepakt worden
 - IPv6 subnetting dient niet om adressen te besparen
 - IPv6 subnetting dient om een logische hierarchie in het netwerk te verkrijgen
 - IPv6 hebben een 48-bit prefix voor subnetting
 - IPv6 moet geen bits lenen

Chapter 10

- Deze layer is dichtst bij de end-user
- Het is de layer die de interface voorziet tussen de application die we gebruiken en de onderliggende layers
- Er zijn verschillende **Application Layer** Protocollen
 - HTTP
 - FTP
 - TFTP
 - IMAP
 - DNS
- De **Presentation Layer** formatteert data voor de Application Layer.
- Deze layer stelt standaarden in voor verschillende bestandstypes.
- Enkele bekende standaarden zijn
 - Quicktime
 - MPEG
 - GIF
 - JPEG
 - PNG
 - etc
- Onder de Presentation Layer ligt de **Session Layer**
- Deze layer maakt en verbreekt sessies tussen de Source en Destination applications.

- Deze layer verworpt de uitwisseling van informatie, houdt de sessie actief en start sessies opnieuw op die onderbroken zijn of gedurende een bepaalde tijd inactief zijn geweest.
- Veel TCP/IP applicaties gebruiken deze 3 layers samen
 - DNS
 - Telnet
 - SMTP
 - DHCP
 - HTTP
 - FTP
 - TFTP
 - BOOTP
 - POP
 - IMAP
- Peer-To-Peer Networking
 - Twee of meer computers zijn verbonden via een netwerk
 - Ze delen resources zoals Printers of bestanden
 - Ieder end-device kan zowel als Server of Client dienen
 - Een voorbeeld thuis kan bijvoorbeeld zijn
 - Twee computers
 - Computer 1 van heeft een Printer via USB aan zich verbonden
 - Computer 2 gebruikt het netwerk om te printen op de printer van Computer 1
 - P2P Applications
 - Ieder device draait een interface en background service
 - Sommige applications gebruiken een hybride systeem
 - Deze gebruiken een index server om te zien welke resource bij welke "peer" opslaan staat
 - Voorbeelden van P2P applications
 - eDonkey
 - eMule
 - Shareaza
 - BitTorrent
 - Bitcoin
 - LionShare
 - Sommigen P2P applications zijn op het Gnutella protocol gebaseerd
 - Mensen delen via dit protocol hun harde schijf met anderen
 - Voorbeelden van dit soort applications zijn
 - BearShare
 - Gnucleus
 - LimeWire
 - Morpheus
 - WinMX
 - XoloX
- Client/Server Model
 - Het apparaat dat data aanvraagt is de Client
 - Het apparaat dat data aanbiedt is de Server
 - Deze processen lopen in de Application Layer
 - Een voorbeeld van dit model is de Email Service van je eigen ISP
 - De email client vraagt aan de Server welke emails ongelezen zijn
 - De server antwoord door deze email naar de client te sturen

- Bekende Application Layer Protocollen
 - Dagelijks gebruik je ongeveer 5 tot 6 Application Layer Protocollen
 - De bekendste zijn
 - HTTP
 - SMTP
 - POP
- HTTP
 - Hypertext Transfer Protocol
 - De browser maakt een verbinding aan van het moment je de URL in de balk typt
 - Web browsers zijn application die een computer gebruikt om deze verbinding te maken
 - De Web servers draaien verschillende services om verschillende bestandstypes aan te bieden
 - De Web server biedt het aangevraagde bestand aan, aan de user
 - De Web browser interpreteert dat bestand en presenteert het aan de user
 - Een Web client opent een pagina op deze manier
 - HTTP Het protocol dat gebruikt wordt
 - www.cisco.com De server naam
 - index.html Het specifieke bestand dat aangevraagd werd
 - Wanneer een web client een aanvraag doet kan deze een Message Type meegeven
 - GET Aanvraag voor data
 - POST Data uploaden (bv een ingevuld formulier op een webpagina)
 - PUT Data uploaden (bv een bestand uploaden)
- HTTP vs HTTPS
 - Dit protocol dient voor beveiligde verbindingen
 - Dit protocol maakt gebruik van authentication en encryption om data versleuteld te versturen
 - Het versleutelen zelf gebeurt via SSL (Secure Socket Layer)
 - Dit soort verbindingen zijn vaak trager door de extra processing time die de Server nodig heeft om de data te encrypteren/decrypteren.
- SMTP/POP
 - POP
 - POP dient om email binnen te halen via een email client
 - **Poort 110**
 - POP3 is aantrekkelijk voor ISPs, berichten worden namelijk niet op een centrale server opgeslaan, maar de client download ze en ze worden verwijderd op de server zelf.
 -
 - SMTP
 - SMTP dient om emails te verzenden via een email client
 - **Poort 25**
 - IMAP
 - Een derde protocol is IMAP, dat extra functionaliteit biedt.
 - IMAP is duurder voor ISPs om te implementeren
 - Er is een centrale backup server nodig
 - IMAP voorziet een mappenstructuur voor emails
 - Emails binnen halen kan dus via POP of IMAP
 - Indien de Email server offline zal de email in een **Spool** geplaatst worden
 - Deze spool zal op een later tijdstip verstuurd worden

- Indien na een bepaalde tijd deze berichten nog altijd niet verstuurd zijn, zal het bericht terug naar de verzender gestuurd worden als "undeliverable".
- DNS
 - Domain Name Service
 - Vormt leesbare web-adressen om in IP-adressen om de verbinding te maken
 - Als een Webmaster beslist om het IP-adres te wijzigen zal deze service de aanpassing naadloos maken voor de end-user.
 - De stappen waarin dit gebeurt
 - De user tikt in zijn web-client een URL in
 - De DNS-server kijkt welk IP-adres er bij die URL hoort (resolving)
 - De DNS-server stuurt het IP-adres terug naar de web-client
 - De web-browser presenteert de inhoud van de webserver op dat IP-adres.
 - Een DNS-server gebruikt het BIND principe om adressen aan te bieden
 - Berkeley Internet Name Domain
 - Dit is ontwikkeld door studenten aan de University of California Berkley in de jaren 80.
 - DNS-servers slaan verschillende "records" om URLs te resoven
 - De types zijn
 - A End-device address
 - NS Authoritative Name Server
 - CNAME Canonical name for an alias (subdomeinen bv)
 - MX Mail Exchange Record
 - Om de DNS recoirds te zien op een Windows Computer
 - **ipconfig /displaydns**
 - DNS Hierarchie
 - Het DNS protocol werkt via het Tree-principe
 - Elke server onderhoudt een specifieke database file en is enkel verantwoordelijk voor die portie
 - Wanneer een DNS-server een request binnen krijgt die niet voor zijn DNS-zone bedoelt is, stuur hij deze request door naar de DNS-server voor de juiste zone.
 - Er zijn dus ook Top-Level Domains
 - .au
 - .co
 - .com
 - .jp
 - .org
 - Na deze volgen Second-Level Domains, etc...
 - Elke Domain Name volgt het path langs de tree-structuur
 - De Root DNS-server weet misschien waar een bepaald DNS-record zit voor een adres (bv. mail.cisco.com), maar het houdt wel de record bij voor het .com domain.
 - De servers die vervolgens de record voor cisco.com bijhouden hebben wel de records voor mail.cisco.com

Enable SSH

- Telnet is not secure.
- It is highly recommended to use SSH for remote shell protocol.
- To configure a Cisco device to support SSH takes four steps:
 - **Step 1.** Ensure that the router has a unique hostname and a IP domain name.
 - **Step 2.** Generate the SSH keys.
 - **Step 3.** Create a local username.
 - **Step 4.** Enable **vtty inbound SSH** sessions.
- The router can now be remotely accessed only by using SSH.



```
R1# conf t
R1(config)# ip domain-name span.com
R1(config)# crypto key generate rsa general-keys modulus 1024
The name for the keys will be: R1.span.com
% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
R1(config)#
*Dec 13 16:19:12.079: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1(config)# username Bob secret cisco
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# transport input ssh
R1(config-line)# exit
```

Step 1: Configure the IP domain name.
Step 2: Generate one-way secret keys.
Step 3: Verify or create a local database entry.
Step 4: Enable VTY inbound SSH sessions.