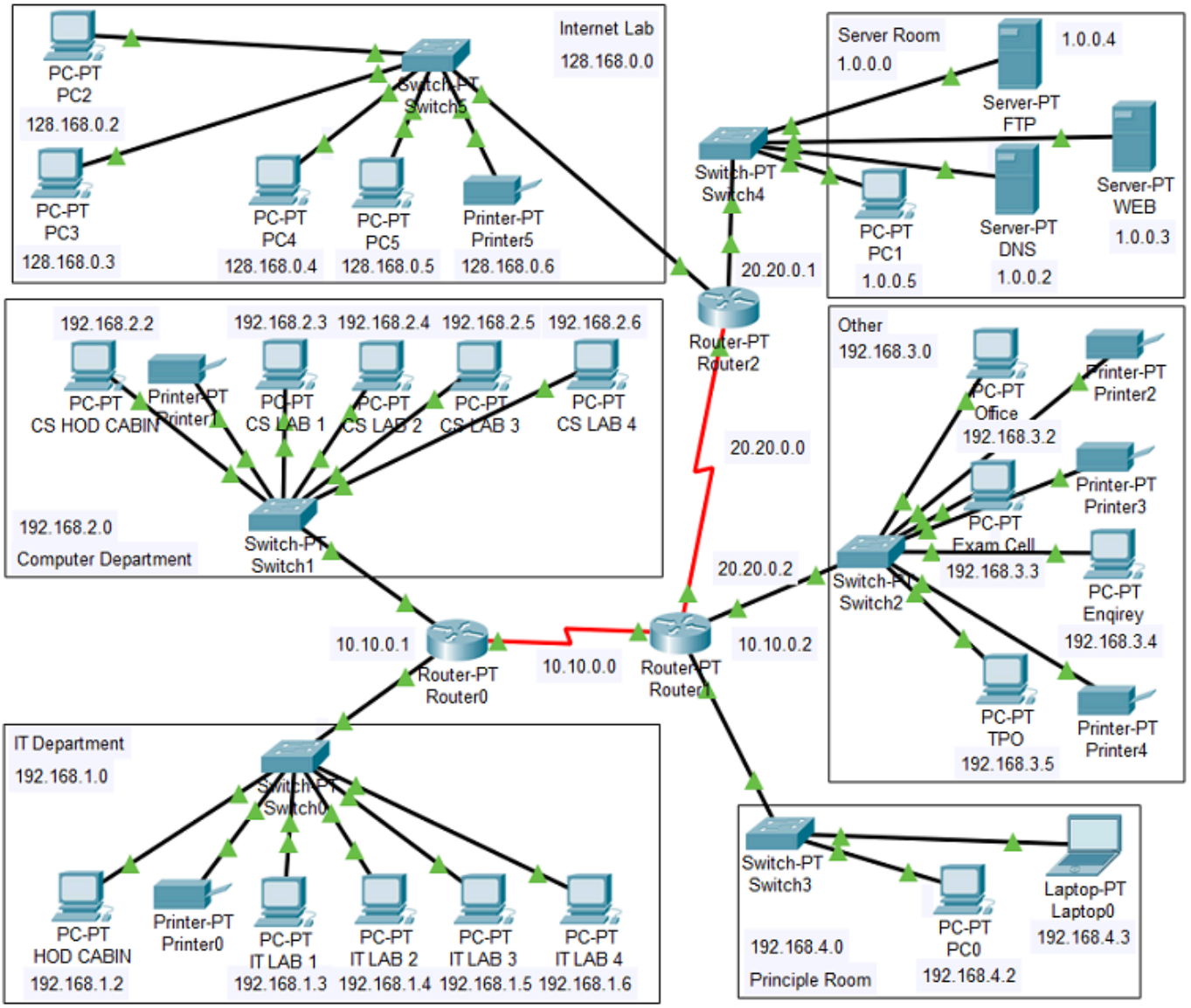
Cisco IOS and Networking

Summary RTSW



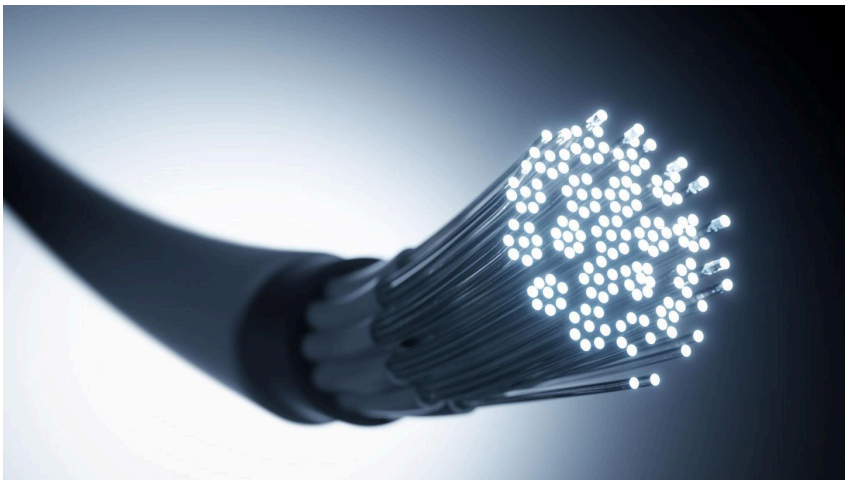
NSE-ICT-2024
Revision 1.5

Daan Breur & Martijn Swarte

If you find anything in this document that is incorrect;
Please send an email to 23052597@student.hhs.nl or 23047399@student.hhs.nl

Nucs
F*ck around and find out

Table of contents



Nucs
F*ck around and find out

Basic Cisco IOS Commands

Modes		
Level	**Mode**	**Promt**
1	User EXEC	`Device>`
2	Privileged Config	`Device#`
3	Global Config	`Device(config)#`
4a	Interface Config	`Device(config-if)#`
4b	Line Config	`Device(config-line)#`

Keyboard Shortcuts	
Up Arrow	Automatically re-types last command
Ctrl+Shift+6	Cancels whatever it's currently doing
Ctrl+C	Exits config mode
Ctrl+Z	Applies current command & returns to priv. EXEC mode
Ctrl+U	Erases anything on current prompt line
Tab	Completes abbreviated command

"Show" Commands	
Command	**Information Displayed**
`show version`	Cisco IOS version, memory capacity, etc.
`show mac address-table`	MAC address table
`show ip route [brief]`	Shows the routing table
`show interface {INTERFACE}`	Status MAC, IP, etc. for the interface
`show interfaces`	Shows all information about all the interfaces
`show ip interface[{s}{brief}]`	Name, IP, status, etc. (all interfaces)
`show running-config`	Shows the entire running config.

Symbol	Description
`Italic font`	Indicates a variable value. you must replace the italicized text.
`[ ]` square brackets	Indicates an optional parameter
`{ }` curly braces	Indicates a non optional parameter
`|` Vertical bars	Separates exclusive choices.
`[{ } { }]` Braces within square bracket	Indicates a choice within an optional element.

Other Commands		
Command	**From Mode**	**Function**
`sdm pre dual def`	Global config	Used if switch won't take IPv6 address
`ip route 0.0.0.0 0.0.0.0 {NEXT_HOP} [WEIGHT:1-255]`	Global config	Set the default route (Gateway of last resort)

General Commands	
Command	**Function**
`enable`	User EXEC > priv. EXEC
`config terminal`	Priv. EXEC > global config
`interface {INTERFACE}`	Global config > interface config
`line`	Global config > line config
`show running-config`	Shows current config
`copy running-config startup-config`	Saves current config
`no ip domain-lookup`	Keeps router from trying to read bad cmds as host names
`erase startup-config`	Erase startup config, must user after labs
`delete vlan.dat`	Erases vlan data, must user after labs
`description {DESCRIPTION}`	To put put a description on an interface or VLAN
`reload`	To reload the operating system
`hostname`	To change the hostname of the system
`ip host {NAME} {IP}`	Adds an entry to the local “dns” resolver (like hosts file on pc)

Nucs
F*ck around and find out

Subnet Cheat Sheet

Subnets

CIDR	Subnet Mask	Addresses	Wildcard
/32	255.255.255.255	1	0.0.0.0
/31	255.255.255.254	2	0.0.0.1
/30	255.255.255.252	4	0.0.0.3
/29	255.255.255.248	8	0.0.0.7
/28	255.255.255.240	16	0.0.0.15
/27	255.255.255.224	32	0.0.0.31
/26	255.255.255.192	64	0.0.0.63
/25	255.255.255.128	128	0.0.0.127
/24	255.255.255.0	256	0.0.0.255
/23	255.255.254.0	512	0.0.1.255
/22	255.255.252.0	1024	0.0.3.255
/21	255.255.248.0	2048	0.0.7.255
/20	255.255.240.0	4096	0.0.15.255
/19	255.255.224.0	8192	0.0.31.255
/18	255.255.192.0	16,384	0.0.63.255
/17	255.255.128.0	32,768	0.0.127.255
/16	255.255.0.0	65,536	0.0.255.255
/15	255.254.0.0	131,072	0.1.255.255
/14	255.252.0.0	262,144	0.3.255.255
/13	255.248.0.0	524,288	0.7.255.255
/12	255.240.0.0	1,048,576	0.15.255.255
/11	255.224.0.0	2,097,152	0.31.255.255
/10	255.192.0.0	4,194,304	0.63.255.255
/09	255.128.0.0	8,388,608	0.127.255.255
/08	255.0.0.0	16,777,216	0.255.255.255
/07	254.0.0.0	33,554,432	1.255.255.255
/06	252.0.0.0	67,108,864	3.255.255.255
/05	248.0.0.0	134,217,728	7.255.255.255
/04	240.0.0.0	268,435,456	15.255.255.255
/03	224.0.0.0	536,870,912	31.255.255.255
/02	192.0.0.0	1,073,741,824	63.255.255.255
/01	128.0.0.0	2,147,483,648	127.255.255.255
/0	0.0.0.0	4,294,967,296	255.255.255.255

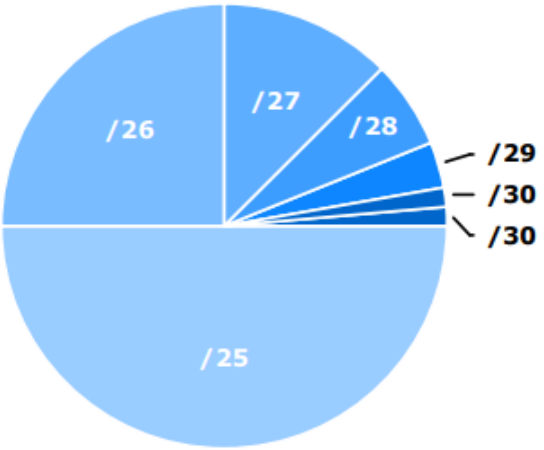
Decimal to Binary

Subnet Mask		Wildcard	
255	1111 1111	0	0000 0000
254	1111 1110	1	0000 0001
252	1111 1100	3	0000 0011
248	1111 1000	7	0000 0111
240	1111 0000	15	0000 1111
224	1110 0000	31	0001 1111
192	1100 0000	63	0011 1111
128	1000 0000	127	0111 1111
0	0000 0000	255	1111 1111

Reserved Ranges

RFC 1918	10.0.0.0 - 10.255.255.255
Localhost	127.0.0.0 - 127.255.255.255
RFC 1918	172.16.0.0 - 172.31.255.255
RFC 1918	192.168.0.0 - 192.168.255.255

Subnet Proportion



CIDR

Classless interdomain routing was developed to provide more granularity than legacy classful addressing; CIDR notation is expressed as /XX keep in mind that the broadcast address and network address Aren't included in the number of hosts

Internet Protocol version 4 (IPv4)

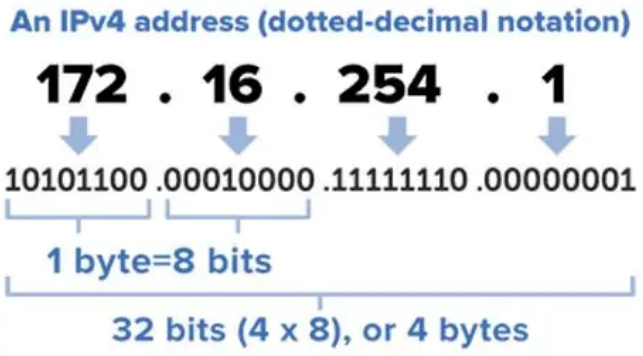
Introduction

IPv4 is the most used Internet Protocol in the world, but it has 1 major flaw; It has a limited amount of available addresses, “only” 4.3 billion(2^32) to be exact. This was once when this protocol was introduced with way too many addresses but nowadays with all the mobile phones etc. it's not enough anymore.

Address structure

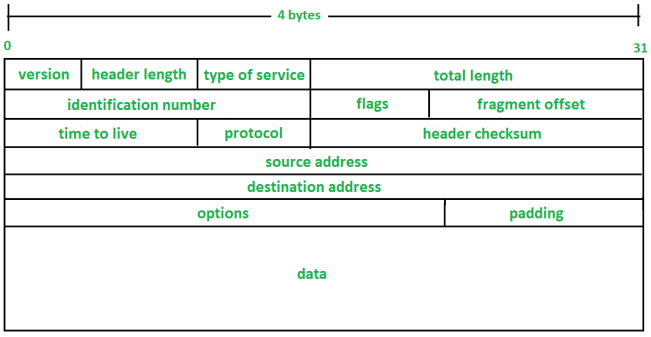
IPv4 has a 4x8bit address structure, it uses a dotted decimal system with 4 so called octets divided by dots. These octets are 8-bit numbers ranging from 0 to 255. As an example;

255.255.255.255



In the IPv4 addresses there is a network and a host portion of the address, this is indicated by either the subnet or the CIDR (This is seen in the chapter “Subnet Cheat Sheet”).

Here’s a quick overview of the IPv4 header information



Internet Protocol version 6 (IPv6)

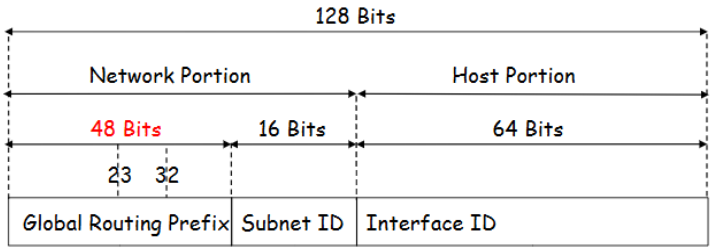
Introduction

Because of the limited number of IPv4 addresses (Only 4.3 billion) there was (and still is...) a need for more addresses so IPv6 was invented. IPv6 can hold up to 3.4 x10^38 different addresses, enough to give every grain of sand its own address

Address structure

IPv6 has a completely different structure from IPv4, instead of using the decimal system it uses the hexadecimal system. IPv6 has 128 bits divided by a semicolon into 8 groups of 16 bits for example;

2001:0DB8:ACAD:0012:0000:0000:0000:0001

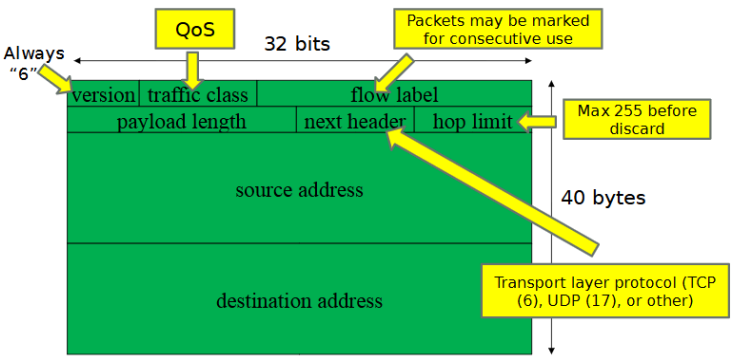


With the new restructuring of IPv6 there are also some new rules for shortening the 128 bits, prefix zero's can be left out and groups of 4 zero's can be left out completely so you get the address like this;

2001:DB8:ACAD:12::1

Which is way easier to work with.

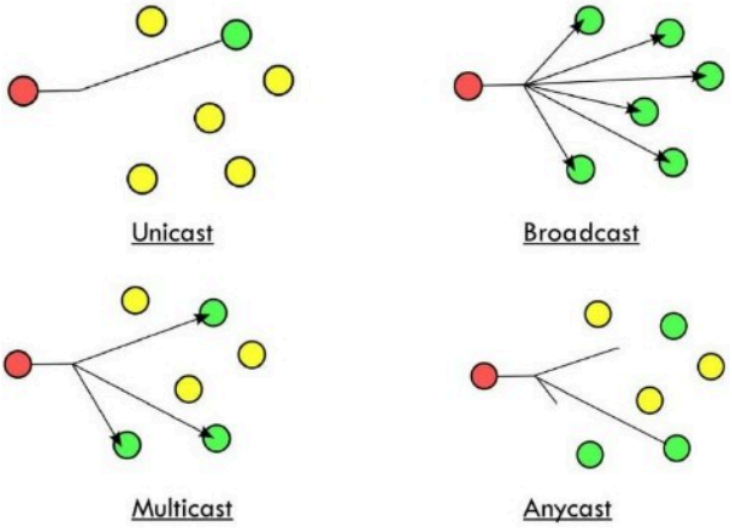
A quick overview of the IPv6 header information.



Address types

There are 3 different address types in IPv6;

- Unicast
  - Addresses a single interface
  - Has 2 different types; global and unique local
- Multicast
  - Are the IPv4's broadcasts.
  - Starts with FF (example; "FF02::/16")
  - Essential for basic IPv6 functionality
- Anycast
  - New to IPv6
  - Addresses a list of devices.
  - Routers decide which of these lists get the packets, can be used for load balancing



Neighbour Discovery Protocol (NDP)

NDP Messages

- Router advertisement (RA); Send by a router to advertise their presence.
- Router Solicitation (RS); Sent by a host to ask a router to send an RA
- Neighbour Solicitation (NS); Send by devices to get the MAC address
- Neighbour Advertisement (NA); Sent as a response to NS messages

Static Routing

Explanation

A router is a device containing two or more ports and is capable of transporting network packets from one port to another and with that one network to the other. Forwarding of networks is done by determining the network information of the packet (mostly L3 network address). Other information (source address, port number) can play a part in the decision if the packet gets to be forwarded or not for the Quality of Service (QoS) and security. In forwarding a packet the frame-header gets changed (source/destination MAC-address) and with that the checksum needs to be recalculated.

Goal of routers

The main goal of routers is to send networking packets to the correct path in the network-topology. In sending the network packets every router makes his own choices. If a router knows something, another router doesn't have to also know it if you haven't told him.

How routers route

Routers function on the network layers L1, L2 & L3. The router receives bits that are passed through to layer 2 where the router "de-encapsulates" the frame (removes the L2 header) and sends the remaining packet to layer 3. In layer 3 the packet is routed based on the destination IP address after which it is "re-encapsulated" and sent through the correct port to the destination.

A small exception is when using NAT, then the router will also change the source address inside of the L3 packet to match the IP of its outgoing interface.

Static Routing

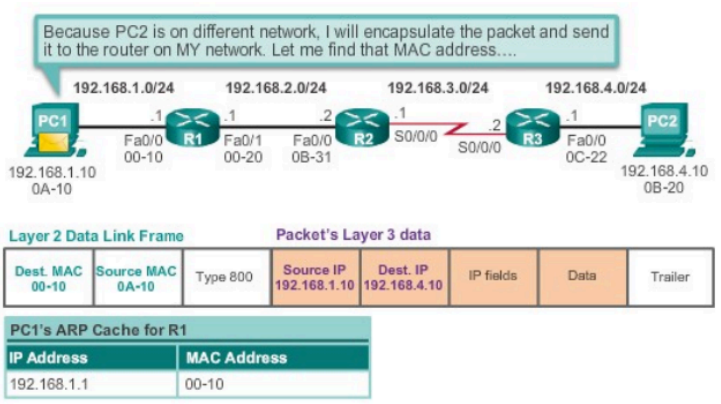
Static routing is the art of manually setting all the routes inside the network to send your packets the correct way.

Commands

Routing Commands		
Command	**Mode**	**Function**
`ip route {NETWORKIP} {SUBNET MASK} {NEXTHOP} [WEIGHT:1-255]`	Global Config	This can be used to set static routes. You can end the command in a weight which tells the router which route to the same network to be prioritized
`show ip route [brief]`	Priv. User	Show a list of all the configured routes
`ip route 0.0.0.0 0.0.0.0 {NEXTHOP} [WEIGHT:1-255]`	Global Config	Configure a gateway of last resort. This is the place that all traffic goes if the routing table does not contain the route.

Route table

A route table is a table you can summon inside the Cisco IOS terminal which will give you an explanation of all the configured routes. With this table you can check if the routes that are configured are the correct ones.



Open Shortest Path First (OSPF)

Explanation

Open Shortest Path First (OSPF) is an Internal Gateway Protocol (IGP) which works together with Link State Routing (LSR) Algorithms in an Autonomous System (AS). OSPF gathers link information from other routers in the network and calculates the shortest path to them. If a link fails OSPF will search for another one.

OSPFv2 is for IPv4
OSPFv3 is for IPv6

Areas

OSPF works on an area basis which will be made inside the network. Area 0 is the backbone to which every other area is linked.

Link State

A link state is the combination of an interface on a router and the corresponding IP address, netmask, the way it is connected and other connected routers. This data is sent as Link State Advertisements (LSA) to all OSPF routers mutually exchanged:

1. When initializing or changing route information, a router sends an LSA (i.e. all Link States)
2. All received LSAs, copy the info to their Link State Database (LSD) and send it through. This is limited to its own area, where each router knows the complete topology
3. On each router the shortest path is determined with the Dijkstra Algorithm

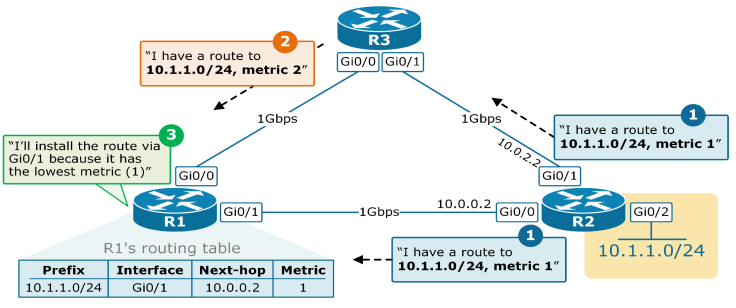
Neighbors

Before routers can exchange LSAs with each other they must see each other as neighbors. This is done using “Hello” messages. “Hello” messages are multicasted every 10 seconds on 224.0.0.5 from an interface running OSPF. If a router gets no “Hello” message for too long he will drop the connection.

Commands

OSPF Show Commands		
Command	**Mode**	**Function**
`show ip ospf interface {INTERFACE}`	Priv. User	Shows OSPF information about a specific interface
`show ip ospf neighbor`	Priv. User	Shows the OSPF neighbor(s)
`show ip ospf database`	Priv. User	Shows the OSPF database, who this router is, routers in our area and their link state
`show ip ospf`	Priv. User	Shows everything about the OSPF

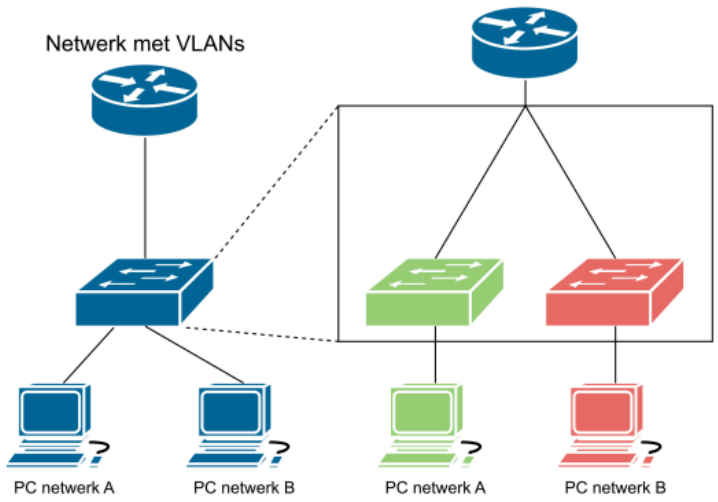
OSPF Config Commands		
Command	**Mode**	**Function**
`Router ospf {PROCESS ID}`	Global config	To go into the OSPF Config.
`ip ospf cost {VALUE}`	Interface Config	With this can set the cost of the path for Dijkstra’s algorithm
`network {NETWORKIP} {WILDCARD} area {AREA}`	OSPF Config	Promotes a network to OSPF
`passive-interface {INTERFACE}`	OSPF Config	Disallows "Hello" packets to be sent to the interface
`router-id {IP}`	OSPF Config	Sets the OSPF callsign of the router, this will be the name of the router in other OSPF routers
`default-information originate`	OSPF Config	This promotes the default gateway to OSPF



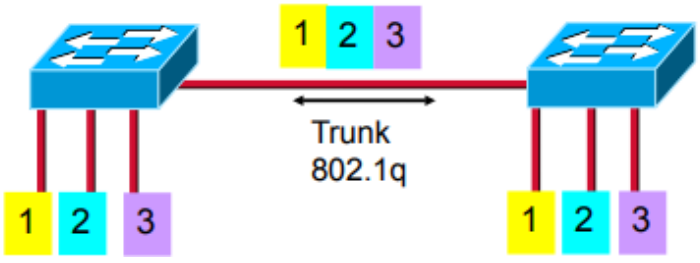
Virtual Local Area Networks (VLANS)

Explanation

If there is a need for more than one network on one location for example if you need different rights for different people then the use of multiple switches is not recommended. For this use case Virtual Local Area Networks (VLANS) were invented.



Each VLAN is kept separate with a number, the VLAN ID. This ID represents that network on the local switch. A switchport is assigned to a VLAN based on that VLAN ID. Every port on a given VLAN ID form their own separate networks with their own Ip, subnet, broadcast domain and default gateway. There is also a separate MAC address table. A pc in one VLAN cannot access a pc in another VLAN without proper routing.



Commands

VLAN Show Commands		
Command	**Mode**	**Function**
`show vlan`	Priv. User	Shows a summary of port-related spanning-tree configuration and status
`show interface trunk`	Priv. User	Shows a summary of all the trunk infaces and the liked VLANS

Trunking

The frames from different VLANS can be sent over one interface to another switch or router with the use of trunking. A trunk is a physical and logical connection between two devices over which multiple VLANS can be transported.

To move VLANS over a trunk there is a need to be able to identify the different VLANS and to what networks they need to go, for this there is a separate protocol called IEEE 802.1q, also known as “Dot 1 q”.

IEEE 802.1q (“Dot 1 q”)

Dot 1 q adds a few bytes to the frame length increasing it from 1518 Bytes to 1522 Bytes, these 4 extra bytes are used to store what protocol is being used and what the VLAN ID is of the packet.

Routing-on-a-stick

VLANS are separated. Without inter VLAN routing a host from one VLAN cannot ping another host on a different VLAN. For this issue there are a few standardized solutions:

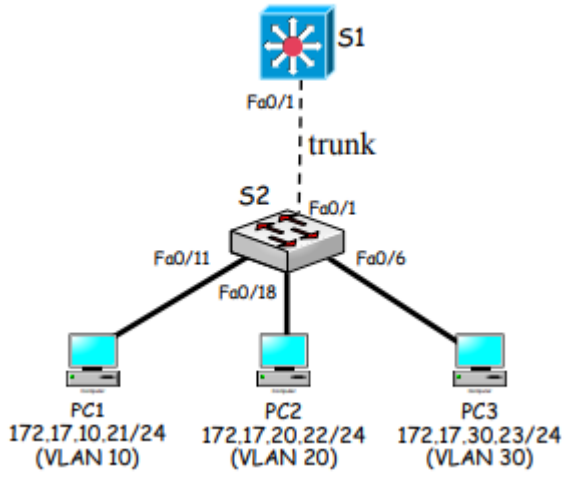
- Every VLAN it’s own kabel to the router
- A trunk with all VLANS to a router (Routing-on-a-stick)
- Multilayer Switch with SVI’s

Virtual Local Area Networks (VLANS)

Switched Virtual Interface (SVI)

A switched virtual interface represents a virtual L3 interface, a VLAN and is also mapped one on one with the VLAN. Every SVI has a VLAN and every VLAN a maximum of one SVI. An SVI has an IP address therefore it can serve as a Default Gateway and can be routed. It can also provide a connection for SSH or as a ping target.

Because an SVI is not associated with a physical interface, multiple L2 connections are used. This is also faster than Routing-on-a-stick. An SVI is sometimes also known as a Routed VLAN Interface (RVI), or simply as a VLAN Interface.



SVI Autostate

A SVI is after configuration only online if:

- The corresponding VLAN is active in the VLAN database on the MultiLayer Switch (MLS)
- The VLAN interface itself has been made and is online (so no shutdown)
- There at least 1 L2 interface available is on the switch with a link to the VLAN. This link cannot be disabled by (STP), it needs to be online.

If these conditions are met the SVI is online. This state of being online is also called SVI Autostate.

Commands

VLAN Config Commands		
Command	**Mode**	**Function**
`delete flash:vlan.dat`	Priv. User	Deletes all the VLAN configs
`vlan {ID}`	Global Config	Gets you to the VLAN Config, only on switches!
`name {NAME}`	VLAN Config	Changes the name of the VLAN so everyone knows what the VLAN does
`interface {INTERFACE}.{VLAN ID}`	Global Config	Goes into VLAN Interface config
`encapsulation dot1q {VLAN ID}`	VLAN Interface Config	To enable IEEE 802.1q (dot1q) encapsulation
`switchport access vlan {VLAN ID}`	Switch Interface Config	To assign a Layer 2 interface to a specified VLAN. only works on interfaces that are operating in access mode
`switchport mode access`	Switch Interface Config	Sets the switchport as an access port
`switchport mode trunk`	Switch Interface Config	Sets the switchport as a trunk port
`no switchport`	Switch Interface Config	Changes a MLS port to a L3 routing port
`switchport trunk encapsulation dot1q`	Switch Interface Config	Sets the encapsulation of the trunk port to dot1q
`switchport trunk native vlan {VLAN ID}`	Switch Interface Config	Changes the native VLAN for a trunk interface from VLAN 1 to the desired VLAN
`switchport trunk allowed vlan {VLAN ID}`	Switch Interface Config	To specify the allowed VLANS on a trunk port

Spanning Tree Protocol (STP)

Explanation

Switching loops can happen and are a problem, the solution for them is the Spanning Tree Protocol (STP). The Spanning Tree Protocol removes loops from a network. The Spanning Tree Algorithm extracts the LAN into a “tree” structure after which the best paths get chosen, not the shortest paths per se and after that the network won’t have anymore loops in it.

Bridge Protocol Data Unit (BPDU)

The Spanning Tree Protocol uses BPDU’s to determine the best paths and to determine which ports to block in order to prevent switching loops.

BPDU Format

The identifier of the BPDU is the BID, the Bridge Identifier, this contains the priority and the MAC-address of a switch. The priority can range from 1 till 32768.

When a switch gets a BPDU packet the lowest priority value wins, not the highest. If the priority values are the same the lowest MAC-address wins.

Priority > MAC-address > port-ID

Working of STP

Spanning Tree Protocol works in three phases, the first phase choosing the root bridge (aka “root war”), the second phase choosing the root ports (the best ports to go to the root bridge) and the last phase choosing the designated ports and disabling the unused ports.

Phase one

Every switch starts up thinking it's the root switch (the most important switch of them all). They send out BPDU packets from every port they have a connection to until they get a BPDU with a lower root-BID value than their own.

- The router will send out BPDU packets with the received BID
- The switch won’t generate anymore BPDU’s
- If the received BPDU is of lower value than their own it will drop the received BPDU.

Commands

STP Show Commands		
Command	**Mode**	**Function**
`show spanning-tree summary`	Priv. User	Shows a summary of port-related spanning-tree configuration and status
`show spanning-tree vlan {VLANID}`	Priv. User	Displays the spanning tree mode and information on the RPVST instance of the specified VLAN

Phase two

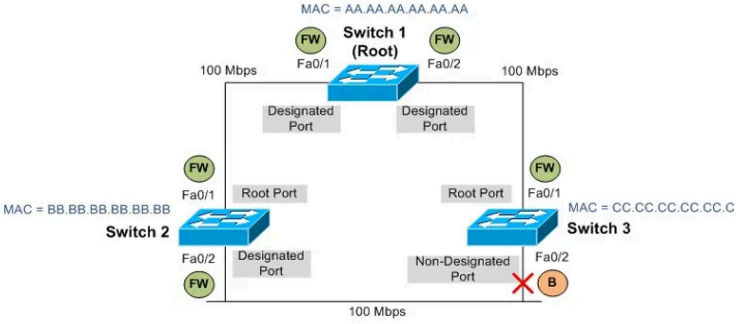
In phase two the non-root bridges need to be chosen, which ports will get used and which won’t. To help with the choosing of the ports the fastest path will get chosen using the root-path-cost.

Root-path-cost

The root-path-cost is a metric to measure distance to the root bridge, every hop the cost is increased with a value that depends on the medium. The port with the lowest root-path-cost becomes the root-port.

Phase three

All ports of the root bridge are designated ports. For the remaining links the sender-BID chooses which ports remain active (designated) and which ports need to be shutdown (blocked). If a switch is connected with two or more links to the same different switch, there will be a loop and the port-ID will determine what port will be shut down (blocked).



Spanning Tree Protocol (STP)

Common Spanning Tree (CST)

STP works on both access and trunk connections between switches. If VLANS are introduced there is only 1 trunk for all the VLANS (1 instance of STP will be started).

Per-VLAN Spanning Tree + (PVST+)

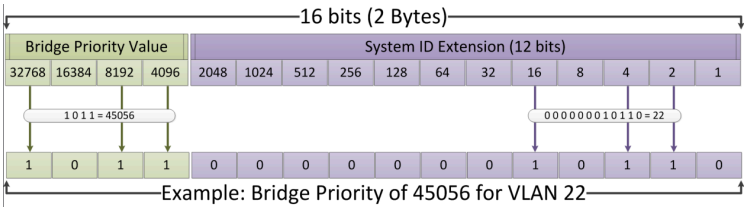
With PVST+ there is one instance of STP per VLAN. The root bridge and with that the blocked ports can be different per VLAN. With this you can achieve a form of load-balancing.

Sending packets

Whereas with STP there is a BPDU packet sent from the switch's MAC (base MAC, not a port MAC) there is a packet sent to 01:00:0C:CC:CC:CD (Shared Spanning Tree). For native VLANS the packets are untagged whereas for other VLANS there is an extra TLV trailer containing the VLAN ID added so PVST+ can keep them apart.

BID

The IEEE standard mandates all BID's be unique. Normally this is done using MAC but this isn't possible with VLANS. Early solutions were the use of multiple MACs but the pool was too small. Now we use system ID extension, in Cisco the VLAN.



PortFast

When plugging a new device into a STP/PVST+ switch it takes 30 seconds (Forward delay) before the port forwards to the device. In an access port for end users STP is not needed, there is no switch. The STP listening/learning traject can be skipped using PortFast, you will need to enable BPDU-Guard to not get any more switching loops when there is a switch connected on accident. BPDU-Guard was made to disable a port when they receive a BPDU on a PortFast port.

Commands

STP Config Commands		
Command	**Mode**	**Function**
`spanning-tree portfast default`	Global Config	enables portfast on access ports
`spanning-tree vlan {VLANID} priority {PRIORITY(lower = better)}`	Global Config	Gives a priority to a spanning-tree vlan, can be used as a form of load balancing
`spanning-tree vlan {VLANID} root {primary/secondary}`	Global Config	Sets a MLS as the root primary or secondary for the specified vlan
`spanning-tree mode {pvst/rapid-pvst}`	Global Config	Sets the mode of the stp, pvst or rapid-pvst
`spanning-tree portfast bpduguard default`	Global Config	Enables bpduguard
`spanning-tree cost {COST}`	Interface Config	Sets the cost of the stp path
`spanning-tree portfast`	Interface Config	Portfast feature causes a switch port to enter the spanning tree forwarding state immediately, bypassing the listening and learning states.
`spanning-tree bpduguard enable`	Interface Config	Blocks bpdu messages on the specified interface

First Hop Redundancy Protocol (FHRP)

Explanation

In a network there are a few aspects that can quite easily be made redundant, L2 switches and routers. With the First Hop Redundancy Protocol (FHRP) we can also make the first hop redundant. This is the hop from a computer to the default gateway and so it is mostly put inside the distribution layer.

First Hop Redundancy Protocols

There are a few different protocols for First Hop redundancy.

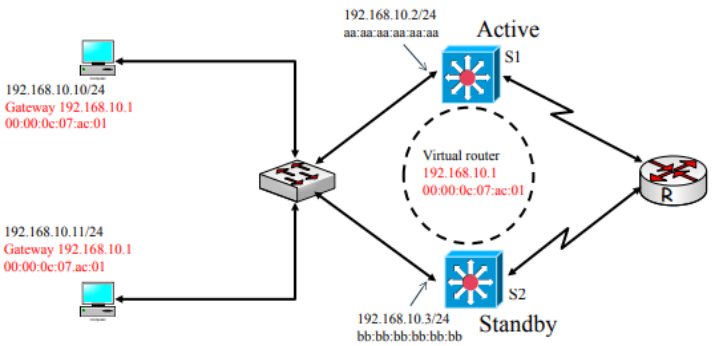
- Hot Standby Routing Protocol (HSRP)
  - Cisco proprietary
- Virtual Router Redundancy Protocol (VRRP)
  - IEEE Standard (Open standard)
  - Lookalike of HSRP
- Gateway Load Balancing Protocol (GLBP)
  - Cisco proprietary
  - Can do load balancing
  - Replaces HSRP

Hot Standby Routing Protocol (HSRP)

Named RFC 2281, HSRP is a Cisco proprietary routing protocol which uses UDP port 1985 on address 224.0.0.2 (version 1) and 224.0.0.102 (version 2) with a TTL of 1. It can provide network redundancy for IP networks, automatic recovery from first-hop failures.

How HSRP works

There are one or more devices working together with each their own IP address but also a shared virtual IP which is used as the default gateway. Only 1 device listens to messages at a time (The active device). If the active device fails for some reason, the standby device takes over. End users don't notice a thing when using HSRP, it could have been one router for all they know.



Commands

HSRP Show Commands		
Command	**Mode**	**Function**
`show standby [brief]`	Priv. user	Shows HSRP information

HSRP Config Commands		
Command	**Mode**	**Function**
`standby {GROUP NUMBER} ip {VIRTUAL IP}`	VLAN Interface Config	Sets the virtual address to use for HSRP
`standby {GROUP NUMBER} priority {PRIORITY[1-255]( Higher = better)}`	VLAN Interface Config	Sets the primary/secondary router priority
`standby {GROUP NUMBER} preempt`	VLAN Interface Config	Attempt to take over as primary router (Can only be done if priority is higher)
`standby {GROUP NUMBER} preempt delay minimum {SECONDS}`	VLAN Interface Config	Puts an extra delay on the preempt command

How HSRP operates

Both devices startup into the initial status, they read thru the configurations and go to the Listening status when they are expecting HSRP-hellos on the network:

- If the Hellos are not received after a time-out period the device who was listening will go into a speak status and chooses a new active- and standby-device by sending each other hello messages.
- If the Hellos are received by the device before the time-out period has gone by the device will stay in listening mode and will be depending on the configured priority be put as Active (highest) or Standby (lowest)

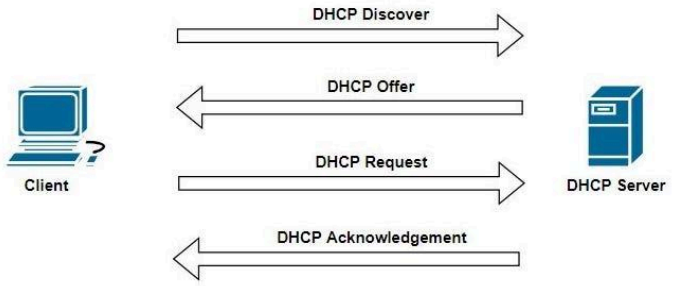
Dynamic Host Configuration Protocol (DHCP)

Explanation

Every device in a network needs an IP address, for this an network admin needs to either; give every computer a static IP address or make a DHCP server which can dynamically address the Ip addresses.

The protocol

DHCP gives Ip related information from a server to an end user, that information is on a lease. As soon as the lease ends the end user needs to request a new Ip or the Ip goes back into the pool of available IPs for other end users. DHCP gives end users other information like the default gateway, the DNS server, the WINS server, the lease term and domain name. Most of the time there is a possibility for static DHCP-Binding where the server gives an IP based on the MAC of the device.



Renewing of lease

When renewing a lease an end user can also ask for a renewal via UDP unicast. A DHCPDISCOVER can also be indicated to receive a broadcast DHCPOFFER for when L2-Unicast is not possible.

DHCP Relay

In a complex hierarchical network, the DHCP server is usually located in a server farm / data center, which is often in another network. A DHCP Relay, also known as an IP Helper Address, allows a router to pass a DHCP broadcast pass to a server elsewhere. This is done by bridging the traffic on the IP of the receiving interface, which then forwards it back to the client.

Commands

DHCP Show Commands		
Command	**Mode**	**Function**
`show dhcp lease`	Priv. user	Shows DHCP information

DHCP Config Commands		
Command	**Mode**	**Function**
`ip dhcp pool {NAME}`	Global Config	Makes a DHCP pool with a name, this will open a submenu for setting
`network {NETWORK_ADDRESS} {SUBNET MASK}`	DHCP Pool Config	Gives the network for which the DHCP pool is meant.
`default-router {IP_DEFAULTGATEWAY}`	DHCP Pool Config	Give the Default-Gateway IP for the given network
`dns-server {IP_DNSSERVER}`	DHCP Pool Config	Give the DNS server for the given network
`domain-name {DOMAIN NAME}`	DHCP Pool Config	Give if relevant the domain name for the given network
`netbios-name-server {IP_NETBIOSSERVER}`	DHCP Pool Config	Give the NetBIOS server for the given network
`ip dhcp excluded-address {IP ADDRESS}`	Global Config	With this command you can keep out ip addresses from the pool the DHCP will give away
`ip dhcp excluded-address {START IP} {END IP}`	Global Config	Same as the other command but you can give a range of IP's
`ip helper-address {DHCP SERVER IP}`	Interface Config	Give on the ip of the DHCP in another network

Access Control List (ACL)

Explanation

A router is a simple packet filter, it forwards or deletes packets based on programmed rules. When a packet arrives at a router with an ACL it will read the necessary information to decide if it permits the packet or denies it, if the packet is denied, it will be thrown away.

Kinds of ACL

There are two kinds of ACL, the standard ACL which just filters based on IP packets on a layer 3 basis and the extended ACL which filters based on source IP/destination IP, source and destination port numbers and protocol type. The way you use a standard or extended ACL depends on the number you provide, 1-99 is for standard ACL, 100-199 is for extended ACL.

Usage of commands

You can use the ACL commands as shown on the right but if you put “ip” in front you can give an ACL for example a name and you go into a submenu where you can instead put in commands.

Rules of ACL

There are two main rules when using an ACL, these are;

1. Standard ACLs need to be as close to the destination as possible, extended ACLs need to be as close to the source as possible.
2. The 3 P’s; 1 ACL per Protocol, per interface and per direction so there is a max of 1 ACL for an interface (in or out) per protocol.

Implicit deny

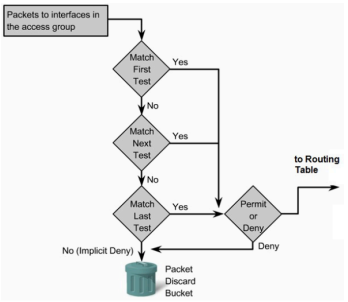
When using ACL the router automatically denies any packets that aren't in the ACL, this is why when making an ACL you put as the last statement (otherwise nothing will work) the command “`access-list 101 permit ip any any`” or change permit for deny, this way others (or yourself in the future) know what the intentions where of the list.

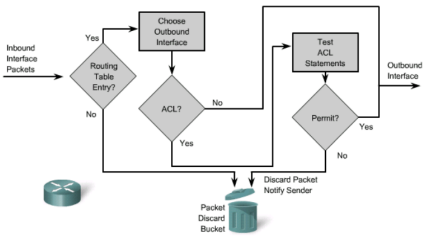
Commands

ACL Show Commands		
Command	**Mode**	**Function**
`show access-list`	Priv. user	Shows ACL information

ACL Config Commands		
Command	**Mode**	**Function**
`access-list {1-199} {[permit/deny]} {IP ADDRESS} {WILDCARD}`	Global Config	Adds a record to the access list, the list will be read from first command to last command
`access-list {NUMBER} [permit|deny] [ip|icmp|tcp|udp] [SOURCE IP] [NETMASK] [eq|ls|gt] [PORT NUMBER|PROTOCOL NAME] [log]`	Global Config	Number is ACL number, ip/icmp/tcp/udp protocol being used, eq/ls/gt (equals, lesser than, greater than), port number/name; the port number or name of process (HTTP, FTP, etc.), log to log the acl usage with command below.
`ip accounting access-violations`	Global Config	Shows the ACL "access-list violation" log
`ip access-group {ACL} {[in/out]}`	Interface Config	Adds an access-list to an interface

Working of ACL





Network Address Translation (NAT)

Explanation

If you want to connect multiple computers to the internet, you will need a public IP. Public IPs are hard to get nowadays and you will likely only get one, but there is a solution; NAT.

The protocol

To work around this we created NAT. A system that, like the name already says, translates network addresses. Inside a network there are the so called private addresses, these addresses are only accessible from within that network. With NAT your router will translate these private addresses to your single (or multiple) public ip addresses.

Types of NAT

There are a couple different kinds of NAT;

- Static NAT; Using static nat you can assign ips 1:1. So you can say this private ip is this public ip. Useful for servers.
- Dynamic NAT; Using Dynamic NAT you can give multiple private IP addresses a fewer number of public IP addresses.
- PAT (Port Address Translation; aka Dynamic NAT with overload); Uses port numbers to translate a lot of private IP addresses to a small number of public addresses (This is what you have at home).

Session Traversal Utilities for NAT (STUN)

- Full Cone NAT: Allows external connections via known destination port. Can use port forwarding.
- Address Restricted Cone NAT: Tracks source port and destination address. Incoming traffic must match these.
- Port Restricted Cone NAT: Like Address Restricted, but incoming source port must also match.
- Symmetric NAT: Translates each source port into a random port. Provides extra security with unique mappings for each destination IP change.

Commands

Nat Show Commands		
Command	**Mode**	**Function**
`show ip nat translations`	Priv. user	Shows the current NAT mappings (NAT Table)
`show ip nat statistics`	Priv. user	Shows a summary of all the nat matches/mismatches
`clear ip nat translation`	Priv. user	Deletes current NAT Table
`debug ip nat`	Priv. user	Generates real-time messages of for example NAT translations

NAT Config Commands		
Command	**Mode**	**Function**
`ip nat pool {POOLNAME} {START PUBLIC IP} {END PUBLIC IP} [prefix/netmask] {PREFIX/NETMASK}`	Global Config	Makes a pool of public IPs for NAT, this is a range of IPs for normal NAT or one IP for PAT.
`access-list {ACL NUMBER} permit {IP INSIDE} {WILDCARD INSIDE}`	Global Config	Makes a standard ACL for the inside network
`ip nat inside source list {ACL NUMBER} pool {POOLNAME} [overload]`	Global Config	Pairs an ACL to a NAT pool, this is mandatory! If using PAT you need to put “overload” behind the command!
`ip nat inside`	Interface Config	Sets an interface to the inside NAT
`ip nat outside`	Interface Config	Sets an interface to the outside NAT
`ip nat inside source static [tcp/udp] {LOCAL IP} {LOCAL PORT} {GLOBAL IP} {GLOBAL PORT}`	Global Config	With this you can "port forward" services when using PAT so people in the outside network can also use them

Other Medium

Explanation

In the world of networking we don't just work with the "normal" connector (RJ45) but also with a few other cables and standards like fiber and serial.

Serial

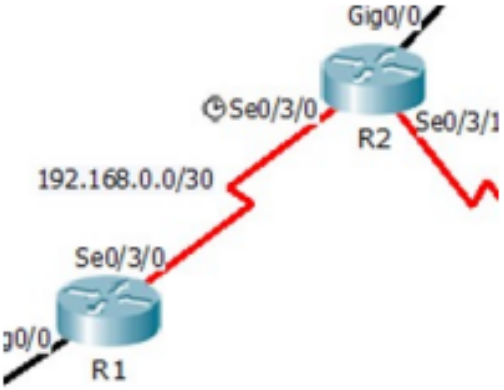
Some interfaces require more configuration than others. In a serial interface there are a few options;

- High-level Data Link Control (HDLC)
- Point-to-Point Protocol (PPP)
- Frame Relay

High-level Data Link Control (HDLC)

HDLC can run synchronously as well as asynchronously. In this document we will only explain the synchronous settings.

HDLC has a Data Circuit Equipment (DCE) and a Data Terminal Equipment (DTE) side. The clock signal gets transmitted from the DCE side, this is mostly an Internet Service Provider (ISP).

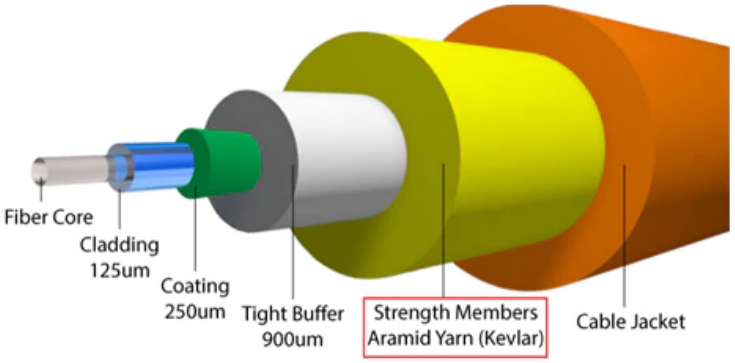


Commands

Other Medium Commands		
Command	**Mode**	**Function**
`clock rate {CLOCK RATE}`	Serial Interface Config	Sets the clock rate on a serial interface (Only available on DCE side)
`udld enable message time 10`	Global Config	Enables UDLD on all ports
`udld aggressive message time 10`	Global Config	Starts UDLD on all ports in aggressive mode.

Fiber optic

With fiber optic and some other Full-Duplex connections (including twisted pair) the detection of L1 errors can be handy. The detection of L1 errors is done with the L2 protocol UniDirectional Link Detection (UDLD).



Aggressive Mode

Aggressive mode is a mode in which fiber can operate. In this mode if 2 fibers are cross linked the wrong way they get turned off. This is done by sending UDLD messages with id data of the neighboring interface of which the message gets on the wrong interface. Also the failing of a line gets noticed and that line will be turned off.

Attachments

Useful Router templates

Keep in mind every template has been made with the password being: “cisco”

Base + SSH

```
en
conf t
hostname {HOSTNAME}
enable secret cisco
no ip domain-lookup
banner motd #No access allowed#
username user priv 15 password cisco
aaa new-model
aaa authentication login MGT local
aaa authentication enable default enable
line vty 0 4
transport input ssh
login authentication MGT
exec-timeout 60
logging synchronous
exit
ip domain-name hhs.nl
crypto key zeroize rsa
yes
crypto key generate rsa general-keys modulus 2048
```

SSH

```
en
conf t
username user priv 15 password cisco
aaa new-model
aaa authentication login MGT local
aaa authentication enable default enable
line vty 0 4
transport input ssh
login authentication MGT
exec-timeout 60
logging synchronous
exit
ip domain-name hhs.nl
crypto key zeroize rsa
yes
crypto key generate rsa general-keys modulus 2048
```

Connection PC to Router using SSH

```
ssh -l user {IP}
```