Table of Contents

Thursday, 24 October 2024 12.55

This Booklet include many of the commands taught in Cisco Academy Program for CCNA courses.

You will also find commands that were helpful to some students, but that you didn't see in the courses.

This is NOT a 'monkey see monkey do' manual but it is up to you to choose which commands to use and when.

BASICS
2-Basics Misc.
3-Basics, CLI, CDP, LLDP …
4-Basic IPv6
5-Password Recovery

SWITCHING
6-Switch, VLAN
7-Trunk, DTP, L3 SW, EtherChannel
8-STP (Spanning Tree Protocol)

SERVICES
9-DHCPv4 (IPv4)
10-DHCPv6 (IPv6)
11-FHRP (HSRP) First Hop Redundancy Protocol
12-NAT

SECURITY
13-Security - general
14-Security - switch
15-ACL (Access Control List)
16-NTP, Syslog, SNMP

ROUTING
17-Inter-VLAN Routing
18-Static Routing, Administrative Distance
19-RIP, RIPng, eBGP
20-OSPFv2 (IPv4)
21-OSPFv3 (IPv6)
22-EIGRP IPv4 - Classic Mode
23-EIGRP IPv6 - Classic Mode
24-Broadband Systems
25-VPNs (GRE, IPsec)

Miscellaneous
26-IOS
27-Virtual PC's - how to connect to LABs

Syntax notes for:

Network

blog: networkmadeeasy.net
YouTube: @NetworkMadeEasy

Basics Misc.

Wednesday, 7 August 2024 13.33

```
!-------------------------------------
! On pc:
!-------------------------------------
arp -a       (show all entries)
arp -d *     (delete all ARP entries)
arp -d <IP> (delete specific entry)
arp -s <IP> <MAC> (insert entry)

netstat -r or
route print (display host routing table)

ipconfig /all
ipconfig /flushdns

!-------------------------------------
! extended ping on PC
!-------------------------------------
ping -t <IP>

!-------------------------------------
! Domain lookup
!-------------------------------------
nslookup <domain>
or
nslookup <ENTER>
> www.google.com
> set type=mx
> cisco.com

!-------------------------------------
! allow icmp traffic through a
! windows firewall
!-------------------------------------
windows firewall
 -> Advanced settings
Inbound Rules
 -> New Rule
Rule Type
 -> Custom
Protocol and Ports
 -> Protocol type = ICMPv4 or ICMPv6
Scope
 -> Which local IP..  = Any IP address
 -> Which remote IP.. = Any IP address
Name
 -> <Give rule a name>
```

```
FTP cmd
ftp ftp.cdc.gov
user: anonymous
pw: blank
ls
get <FILE>
quit
more <file>

FTP program
WS_FTP LE
http://www.wsftple.com/download.aspx

FTP in browser
ftp://ftp.cdc.gov
```

```
subnet calculators:
www.solarwinds.com.
linux - yum install ipcalc
web based www.ipcalc.org
```

```
www.rfc-editor.org
www.macvendorlookup.com
```

```
install telnet client on win7
pkgmgr /iu:"TelnetClient"
```

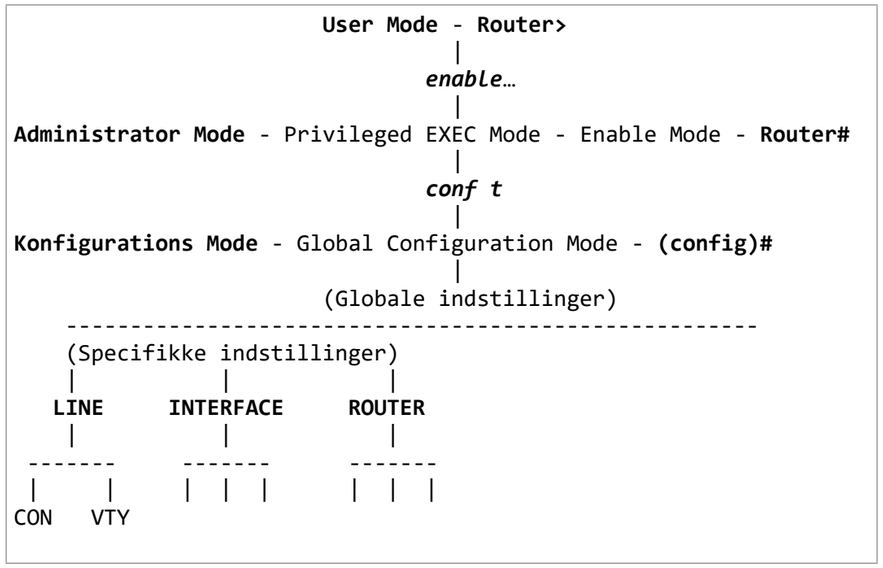
```
Wireshark
    -filter (icmp, arp, tcp, dns, ftp, tftp, ssh)
    -Edit-Preferences-UDP-Validate UDP checksum if possible
    -tcp and ip.addr==<IP>
    -Go - next packet in conversation
    -right click tcp packet - follow TCP stream

Wireless NIC
```

```
Misc. terms:
    • how to use terminal program with logging
    • TCP 3-Way handshake
    • IoE (The Internet of Everything)
    • basic switch function
    • basic routing function
```

Basics, CLI, CDP, LLDP …

Saturday, 24 August 2024 14.26

```
!-------------------------------------
! Connect to the router/switch:
!-------------------------------------
Console settings:
  9600 bps
  Data bits: 8
  Stop bits: 1
  Parity: none
  Flow control: none

!-------------------------------------
! Basics
!-------------------------------------
! Administrator mode:
enable

! Basic clock config:
clock set…

! Save config:
copy running-config startup-config
or
write

! Erase the startup configuration file from NVRAM:
erase startup-config


! Configuration mode
configure terminal

! Hostname…
hostname <>
no ip domain-lookup

! 'mini' DNS
ip host <HOSTNAME> <IP-1> <IP-2>

!-------------------------------------
! Interface
!-------------------------------------
int <>
 description <>
 bandwidth <Kbps>
 ip address <ip> <sm>
 no shutdown
 exit

!-------------------------------------
! DCE interface
!-------------------------------------
int serial <>
 clock rate [speed]



remember to add no shutdown on interfaces when copying back
to equipment
```




```
!-------------------------------------
! CDP/LLDP
!-------------------------------------
sh cdp
sh cdp entry <>
sh cdp interface [detail]
sh cdp traffic
no cdp run ! Turn CDP off globally
cdp enable ! Enable CDP on specific interface

lldp run ! Turn LLDP on
sh lldp
sh lldp run
no lldp transmit|receive ! On specific interface
sh lldp entry
sh lldp neighbors
```

```
!-------------------------------------
! Basic Show commands
!-------------------------------------
show version
sh file systems
sh running-config
sh ip interface brief
sh clock
sh cdp neighbors [detail]
sh interfaces <>
sh interfaces description
sh protocols
sh arp | sh ip arp
sh flash or dir flash:
sh ip route

!-------------------------------------
! Pipe commands
!-------------------------------------
sh ver | include <word>
sh startup-config | begin vty
sh run | section ip route

sh run | section line vty
sh ip int brief | include up
sh ip int brief | exclude unassigned
sh ip route | begin Gateway
```

```
!-------------------------------------
! extended ping in CLI
!-------------------------------------
ping <ENTER>
ping <IP> repeat 500

ping -n 25 www.afrinic.net > afrinic.txt
more afrinic.txt
dir *.txt
```

Traceroute tools:

```
ping <IP>
traceroute/tracert <IP>
```

Web tool:
http://www.subnetonline.com/pages/network-tools/online-traceroute.php

Visual tool:
http://www.visualroute.com/download.html

Copy commands:

```
copy flash: tftp:
copy running-config tftp:
copy tftp: running-config
copy running-config flash:
more flash:<text-file>
copy running-config usbflash0:
```

Afbryd sekvens:
ctrl-c

ctrl-shift-6 [x]

(*On MAC use US keyboard*)

```
!-------------------------------------
! Initializing and Reloading a Router and Switch
!-------------------------------------
enable
erase startup-config
[delete vlan.dat]
reload
```

```
!-------------------------------------
! Command History Feature
!-------------------------------------
terminal history size 200
sh history
```

Basic IPv6

Monday, 25 March 2024 15.00

```
!-----------------------------------------
! enable IPv6 routing
!-----------------------------------------
ipv6 unicast-routing

sh ipv6 int <>

!-----------------------------------------
! IPv6 on interface
!-----------------------------------------
int <>
 description <>
 ipv6 address <>/64
 no shutdown

!-----------------------------------
! change the link-local address
!-----------------------------------
interface s1/0
 ipv6 address FE80::1 link-local

ping FE80::1
show ipv6 interface serial 1/0

cisco best practice is to manualy assign the link-local
address

!-----------------------------------
! Configure EUI-64 address
!-----------------------------------
interface fa 0/0
 ipv6 address <>/64 eui-64

show ipv6 interface fa 0/0
sh ipv6 interface brief


!unique-local addres recommended for p2p ser
int <ser>
 ipv6 address FC00::1/64
 no shut
```

IPv6 SLAAC
(Stateless Address Autoconfiguration)

By default, Cisco routers send RA messages every 200 seconds. RA messages are always sent to the **IPv6 all-nodes multicast address** FF02::1

Router Solicitation (RS)- Search
(ff02::2 - **to all-routers** - ICMPv6 type 133)

Router Adverticement (RA)- Inform
(ff02::1 - **to all-nodes** - ICMPv6 type 134)

Neighbor Solicitation (NS)- Search
(ICMPv6 type 135)

Neighbor Adverticement (NA)- Inform
(ICMPv6 type 136)

```
ping -6 <> !ipv6 ping
```

IPv6:
128bit
8 hextet's or 8 '16-bit segments'
N:N:N:N:H:H:H:H/64 (Net:Host)

::1 (**loopback address**)
FE80:… (**link-local address**)

all routers multicast group (FF02::2**)**
This will allow the PCs to obtain their IP address and default gateway information automatically using Stateless Address Autoconfiguration (SLAAC).

anycast address
Used to facilitate load sharing and provide alternate path flexibility if a router becomes unavailable. An IPv6 unicast address that is assigned to multiple devices. A packet sent to an anycast address is routed to the nearest device that has that address.

Site-local address (deprecated)
site-local addresses have been *deprecated* and replaced by unique-local addresses.
Site-local addresses were identified by the numbers **FEC0** in the initial hextet.

Unique Local address
FC00::/7 - FDFF::/7
Have some similarities to RFC1918

Link-local address
FE80::/10

GUA (Global Unicast Address)
2000::/3

Multicast address
FF00-FFFF

The IPv6 global prefix 2001:DB8::/32 is a reserved prefix for use in documentation, as described in RFC 3849.

The default bias template used by the Switch Database Manager (SDM) does not provide IPv6 address capabilities. Verify that SDM is using either the '**dual-ipv4-and-ipv6**' template or the '**lanbaserouting**' template. The new template will be used after reboot even if the config is not saved.

```
S1# show sdm prefer

Follow these steps to assign the dual-ipv4-and-ipv6
template as the default SDM template:
S1# configure terminal
S1(config)# sdm prefer dual-ipv4-and-ipv6 default
S1(config)# end
S1# reload

sdm prefer [default|dual-ipv4-and-ipv6|lanbase-routing|qos]
2960 supports up to 750 static routes

sdm prefer lanbase-routing
!remember to reload switch
```

Password Recovery

Monday, 22 August 2022 14.48

```
!-------------------------------------
! Password Recovery - Router
!-------------------------------------
config-register|confreg
0x2102|0x2142
reset
alt+b in Tera Term -> ROMMON
CTRL-Break in PUTTY -> ROMMON

To recover or reset the enable password on the
Cisco 1900 series router, complete the following
steps:
   1. Establish a terminal connection with the
      router using Tera Term or other terminal
      emulator.
   2. Boot to ROMMON by either removing flash and
      rebooting or selecting Alt-b during a reboot.
   3. Type confreg 0x2142 at the rommon prompt.
   4. Type reset at the next rommon prompt.
   5. Type no at the initial configuration dialog.
   6. Type enable at the router prompt.
   7. Type copy startup-config running-config to
      load the startup configuration.
   8. Type show running-config.
   9. Record an unencrypted enable password. Reset
      an encrypted enable password.
  10. In configuration mode, type config-register
      0x2102.
  11. In privilege mode, type copy running-config
      startup-config in order to save configuration.
  12. Use the show version command to verity
      configuration register settings.
```

```
!-------------------------------------------------------
! Password Recovery - Switch
!-------------------------------------------------------
press MODE button (within 15 seconds after power on)
 - LED flashing green
 - LED turns briefly amber and then solid green
 - release the Mode button

 follow instruction

   1. flash_init
   2. [load_helper]
   3. rename flash:config.text flash:config.text.old
   4. boot
   5. rename flash:config.text.old flash:config.text

!-------------------------------------------------------
! Manage IOS and Config on Switch
!-------------------------------------------------------
sh version
sh flash
cd flash:/<dir>

copy flash tftp
copy tftp flash

copy startup-config tftp
erase nvram
copy tftp startup-config

sh bootvar (old cmd sh boot)
rename flash:/… flash:/
dir flash:/

delete flash:/…/html/*

archive tar /x tftp://<ip-of-tftp>/<ios-name> flash:/<dir>

boot system flash:/path/IOSname
```

Switch, VLAN

13. februar 2023 14:14

```
!------------------------------
! show commands
!------------------------------
sh ip int brief
sh interface <vlan-id>
sh interface <> [status]
sh vlan [brief]
sh vlan summary
sh vlan name <>
sh vlan id <>
dir flash:
sh flash:

!-----------------------------------
! speed settings on ports
!
! Link Speed: determined by electrical signaling
! Duplex mode: negotiated through an exchange of
!  information
! If autonegotiation fails (10/100Mb)
!  - fallback default is 'half-duplex'
! If autonegotiation fails (1000Mb)
!  - fallback default is 'full-duplex'
! Functions only if BOTH ENDS are set to
! AUTONEGOTIATION!!!
!-----------------------------------
int fa 0/x
 speed {auto|100}
 duplex {auto|full}

 mdix auto
 sh controllers ethernet-controller <> phy | include Auto-MDIX
!-----------------------------------
! Management module in Layer 2 switch
! SVI (Switched Virtual Interface)
!-----------------------------------
vlan <management-vlan>
 exit
int vlan <management-vlan>
 ip address <net> <sm>
 no shutdown
 exit
ip default-gateway <gateway-ip-for-management-vlan>

!-----------------------------------
! Set one or more ports in management-vlan
!-----------------------------------
int range fa0/1 - 24 , gi0/1 - 2
 switchport mode access
 switchport access vlan <management-vlan>
 exit

!-----------------------------------
! Create VLANs
!-----------------------------------
vlan <vlan-id>
 name <name>

!-----------------------------------
! VLAN on port
!-----------------------------------
int range fa 0/x - y
or
int range fa 0/x, fa0/y, fa0/z
 description ...
 switchport mode access
 switchport access vlan <vlan-id>
```

```
!------------------------------
! Clear Switch
!------------------------------
delete vlan.dat
erase startup-config

Check: sh vlan

If previous VLAN configuration information is still
present (other than the default management VLAN 1), you
must power-cycle the switch (hardware restart ) instead of
issuing the reload command. To powercycle the switch,
remove the power cord from the back of the switch or
unplug it, and then plug it back in.

power cycle or reload


!------------------------------
! Reset interface to default settings
!------------------------------
default int <>
```

```
!------------------------------
! Data and Voice VLANs
!------------------------------
vlan <>
 name DATA
vlan <>
 name VOICE

Int <>
 switchport mode access
 switchport access vlan <>
 mls qos trust cos
 switchport voice vlan <>
```

Trunk, DTP, L3 SW, EtherChannel

Monday, 22 August 2022 16.52

```
!-------------------------------------
! Create trunks (802.1Q)
!-------------------------------------
int range fa 0/x - y
 switchport trunk encapsulation {dot1q|isl}
 switchport mode {trunk|dynamic auto|dynamic desirable}
 switchport trunk native vlan <vlan-id>
 switchport trunk allowed vlan x,y,a - b
 switchport nonegotiate ! turn off DTP
 no shutdown

! reset trunk to default
 no switchport trunk allowed vlan
 no switchport trunk native vlan

sh int trunk
sh int <> switchport
sh run int <>
sh dtp interface <>
```

VLAN 1 carry control protocols: DTP, VTP, STP BPDUs, PAgP, LACP, CDP…
from IOS 12.1(11b) VLAN1 can be removed from trunk and control protocols continue to flow on VLAN1

```
!-------------------------------------
! EtherChannel
!-------------------------------------
Fast EtherChannel (FEC) - bundle ports
FEC – up to 8 100Mb full duplex (1.6Gb)
GEC – up to 8 1Gb full duplex (16Gb)

PAgP - Cisco proprietary
LACP - 802ad - non-Cisco devices
```

PAgP	LACP 802.3ad	Negotiation packets sent?	
on	on	No	All ports channeling
desirable	active	yes	actively asks to form a channel
auto	passive	yes	waits to channel , until asked

```
!-------------------------------------
! Connect with Cisco equipment (PAgP):
!-------------------------------------
int range fa x/x – y
 shutdown !! no shutdown AFTER ALL config is done on Port-Channel
  channel-group 1 mode {on|off|desirable|auto}

!
int port-channel 1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk allowed vlan <x,y,z>

!-------------------------------------
! Connect with non-Cisco equipment (LACP):
!-------------------------------------
int range fa x/x – y
 shutdown !! no shutdown AFTER ALL config is done on Port-Channel
 channel-group 1 mode {on|off|active|passive}
!
int port-channel 1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk allowed vlan <x,y,z>


sh etherchannel summary
sh etherchannel port-channel
sh int port-channel <>
sh int <> etherchannel
sh run int <>

Check if port is in err-disabled
- shutdown and no shutdown
```

```
!-------------------------------------------------
! Dynamic Trunking Protocol (DTP)
! Cisco proprietary
!-------------------------------------------------
```

Mode	Negotiation packets sent?		
trunk	yes	active	permanent trunking mode
access	yes	active	permanent non-trunking mode
desirable	yes	active	actively asks to form a trunk
auto	yes	passive	access; but can trunk *if asked*
nonegotiate	no		no DTP (only in trunk and access mode)

```
!-------------------------------------
! Layer 3 port on Layer 3 switch
!-------------------------------------
ip routing !turns ipv4 routing on

interface <>
 no switchport
 ip address x.x.x.x
exit
```

STP (Spanning Tree Protocol)

23. maj 2023 14:28

```
!-----------------------------------------------
! Spanning-tree (STP)
!-----------------------------------------------
spanning-tree mode {pvst|rapid-pvst} ! on all switches

!--------------------------------------
! Choose root switch
!--------------------------------------
! using wizzard
! spanning-tree vlan <vlan-id's> root {primary|secondary}
! primary = 32768-8192 = 24576
! secondary = 32768-4096 = 28672
!
!or do it manually
spanning-tree vlan <vlan-id's> priority <no>
! 32768 default priority
! increments of 4096
! 4096 -> root
! 16384 -> secondary root

!--------------------------------------
! Enable portfast/Edge and BPDU Guard
!--------------------------------------
spanning-tree portfast default
! enables PortFast on all nontrunking ports
spanning-tree portfast bpduguard default
! enables BPDU guard on all PortFast ports
!
or
int fa 0/x
 spanning-tree portfast
 spanning-tree bpduguard enable

!--------------------------------------
! Change root port using spanning-tree cost
!--------------------------------------
int <>
 spanning-tree cost <no>

sh spanning-tree [vlan <vlan-id>]
sh spanning-tree summary
sh spanning-tree interface…
sh spanning-tree inconsistentports
sh running-config | include spanning-tree mode

debug spanning-tree events
```

```
!--------------------------------------
! 3 steps for STP units
!--------------------------------------
   1. Elect The Root (The one with the lowest BID)
   2. Find the best path to the root
      Elect Root ports (according to 4 step decision
      sequence)
   3. Block whatever is left over
      Elect Designated ports (according to 4 step
      decision sequence)
      The other end of cable is blocking

!--------------------------------------
! 4 step decision sequence
!--------------------------------------
   1. Lowest Path Cost to root bridge
   2. Lowest sender BID
   3. Lowest sender Port priority
   4. Lowest sender Port ID
```

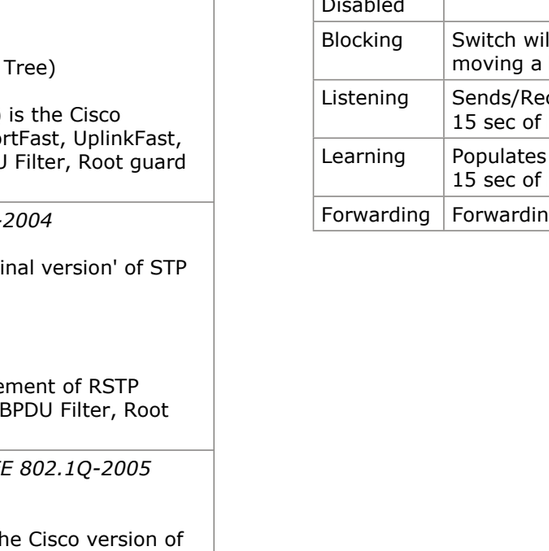
802.1D-1998	STP	*Deprecated version* The 'original version' of STP BPDU originate from root Use timers Makes a CST (Common Spanning Tree) PVST+ (Per-VLAN Spanning Tree) is the Cisco enhancement of STP (supports PortFast, UplinkFast, BackboneFast, BPDU Guard, BPDU Filter, Root guard and Loop guard)
802.1w	RSTP	*Now integrated into IEEE 802.1D-2004* Faster convergence than the 'original version' of STP Don't use timers but uses handshakes Uses 'Long Path Cost' Rapid PVST+ is the Cisco enhancement of RSTP (supports PortFast, BPDU Guard, BPDU Filter, Root guard and Loop guard)
802.1s	MSTP	*Now an integrated part of the IEEE 802.1Q-2005 standard* MST (Multiple Spanning Tree) is the Cisco version of MSTP
802.1D-2004	RSTP	Now uses RSTP and the 'old' IEEE 802.1w is now deprecated Don't use timers but uses handshakes As default Cisco uses Short Path Cost

Link speed	IEEE 802.1D-1998 STP	IEEE 802.1D-2004 RSTP
Mb	Short Path Cost	Long Path Cost
10	100	2.000.000
100	19	200.000
1.000	4	20.000
10.000	2	2.000

802.1D		**802.1w**
Disabled		Discarding
Blocking	Switch will wait up to 20 sec (max-age) before moving a blocked port into listening phase	Discarding
Listening	Sends/Receives BPDU 15 sec of listening for BPDUs	Discarding
Learning	Populates switch CAM table 15 sec of learning MAC addresses	Learning
Forwarding	Forwarding traffic	Forwarding

```
(config)#spanning-tree udld enable
(config-if)#spanning-tree udld enable
```

```
(config-if)#spanning-tree guard root
```




```
(config)#spanning-tree loopguard default
 or
(config-if)#spanning-tree guard loop
```

```
(config)#spanning-tree portfast bpduguard default
 or
(config-if)#spanning-tree bpduguard enable
```

```
(config-if)#spanning-tree portfast
```

Protecting against **unexpected** BPDUs

Protecting against **sudden loss** of BPDUs

Root guard: Apply to ports where root is never expected. -> root-inconsistent

BPDU guard: Apply to all user ports where PortFast is enabled. -> errdisable

Loop guard: Apply to nondesignated ports but okay to apply to all ports.

UDLD: Apply to all fiber-optic links between switches (must be enabled on both ends).

Permissible combinations on a switch port:

Loop guard and UDLD
Root guard and UDLD

Not permissible on a switch port:

Root guard and Loop guard
Root guard and BPDU guard

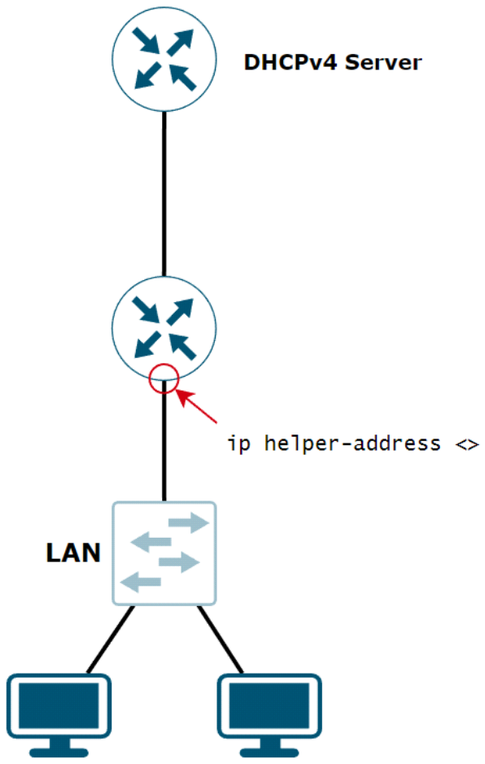
DHCPv4 (IPv4)

Monday, 29 July 2024 14.16

Dynamic Host Configuration Protocol (**DHCP**)

Discover, Offer, Request, Acknowledgement (DORA)

```
!--------------------------------------------
! Stateful DHCP Server (IPv4)
!--------------------------------------------
!service dhcp is enabled by default
service dhcp !also enables relay agent function

ip dhcp excluded-address <start-IP> [<end-IP>]
ip dhcp pool <NAME>
 network <net> <sm>
 dns-server <dns-IP>
 default-router <gw-IP>
 domain-name <>
 lease <days>

sh ip dhcp binding
sh ip dhcp pool
debug ip dhcp server events
sh ip dhcp server statistics
sh ip dhcp conflict
sh run | section dhcp

!--------------------------------------------
! relay agent
!--------------------------------------------
interface fa 0/0
 ip helper-address <dhcp-IP>

sh ip int <>
sh ip helper-address


!
```



DHCPv6 (IPv6)

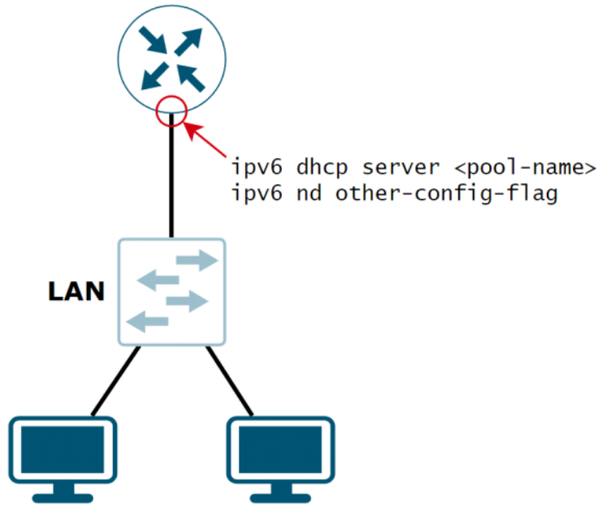
Thursday, 24 October 2024 10.23

Dynamic Host Configuration Protocol (**DHCP**)

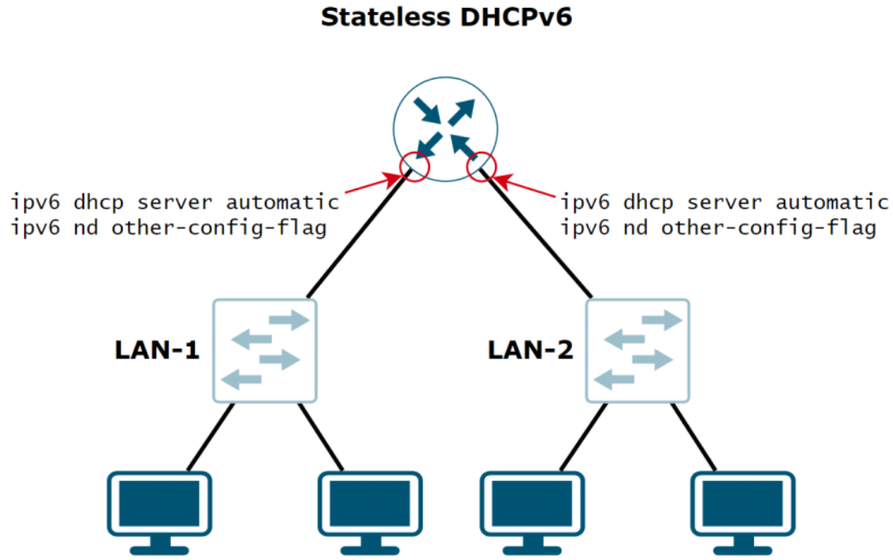
(RS), RA, Solicit, Advertise, Request, Reply

```
!-------------------------------------
! Stateless DHCP Server (IPv6)
!-------------------------------------
ipv6 unicast-routing !make the router able to source RA messages
!
ipv6 dhcp pool <name>
 [link-address <relay-agent-IP>] !only if 'ipv6 dhcp server automatic'
 dns-server <>
 domain-name <>
!
int <>
 ipv6 dhcp server <pool-name>  !bind the dhcpv6 pool to an interface
 ! Set nd flags (A, M, O) on client gateway interface
 ipv6 nd other-config-flag     !O flag = 1 - use stateless dhcp
                               !A flat = 1 - default setting

!-------------------------------------
! use router as Stateless DHCPv6 Client
!-------------------------------------
int <>
 ipv6 enable
 ipv6 address autoconfig !use SLAAC

sh ipv6 dhcp int <>
sh ipv6 int <>

!-------------------------------------
! Stateful DHCP Server (Packet Tracer ikke stabil)
!-------------------------------------
ipv6 unicast-routing !make the router able to source RA messages

ipv6 dhcp pool <name>
 address prefix <ipv6-prefix> [lifetime {<time>|infinite}]
 dns-server <>
 domain-name <>

int <>
 ipv6 dhcp server <pool-name>          !binds the dhcpv6 pool to an interface
 ipv6 nd prefix default 1800 1800 no-autoconfig  !A flag = 0
 ipv6 nd managed-config-flag                     !M flag = 1

sh ipv6 dhcp pool
sh ipv6 dhcp binding
sh ipv6 int <>

!-------------------------------------
! use router as Stateful DHCPv6 Client
!-------------------------------------
ipv6 unicast-routing

int <>
 ipv6 enable
 ipv6 address dhcp  !use dhcpv6

!-------------------------------------
! DHCPv6 relay agent
!-------------------------------------
!int <>
 ipv6 dhcp relay destination <server IP> <egress int>
 end

sh ipv6 dhcp int <>
```

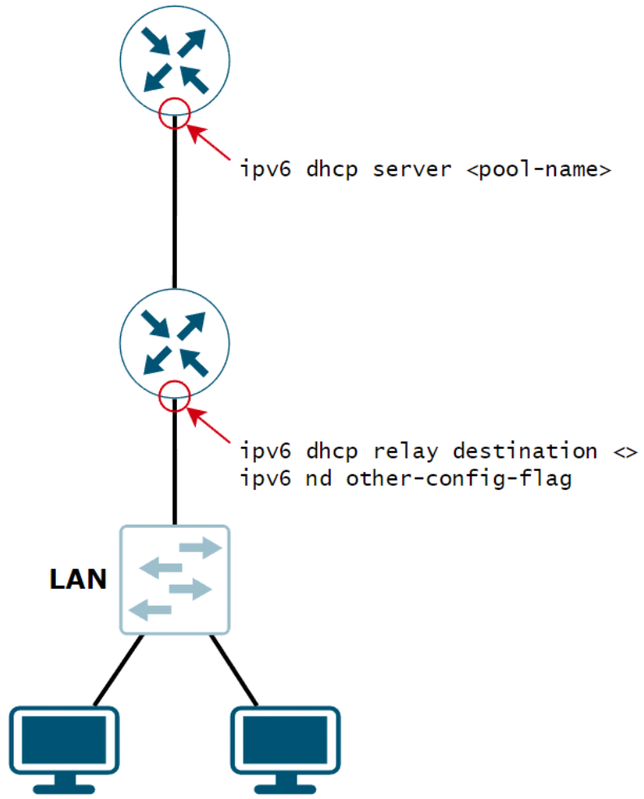
Stateless DHCPv6



Stateless DHCPv6



Stateless DHCPv6




```
debug ipv6 dhcp detail

ff02::1:2 - All DHCPv6 Agents
```

Flags in RA (Router Advertisement)

A Autonomous	M Managed	O Other	Function
1 (default)	0 (default)	0 (default)	SLAAC (Stateless Address Autoconfiguration) - IPv6, Default Gateway
1	0	1	Stateless DHCPv6 - Domain, DNS IP
0 *	1	0	Stateful DHCPv6 - IP, Domain, DNS IP …

* If A=1 and M=1, some OS i.e. Windows will create an IPv6 address using SLAAC and also obtain an address from the stateful DHCPv6 server. *In most cases it is recommended to manually set A=0*

```
!-------------------------------------
!reset M & O flag to default ('0')
!-------------------------------------
no ipv6 nd managed-config-flag
no ipv6 nd other-config-flag
```

FHRP (HSRP) **First Hop Redundancy Protocol**

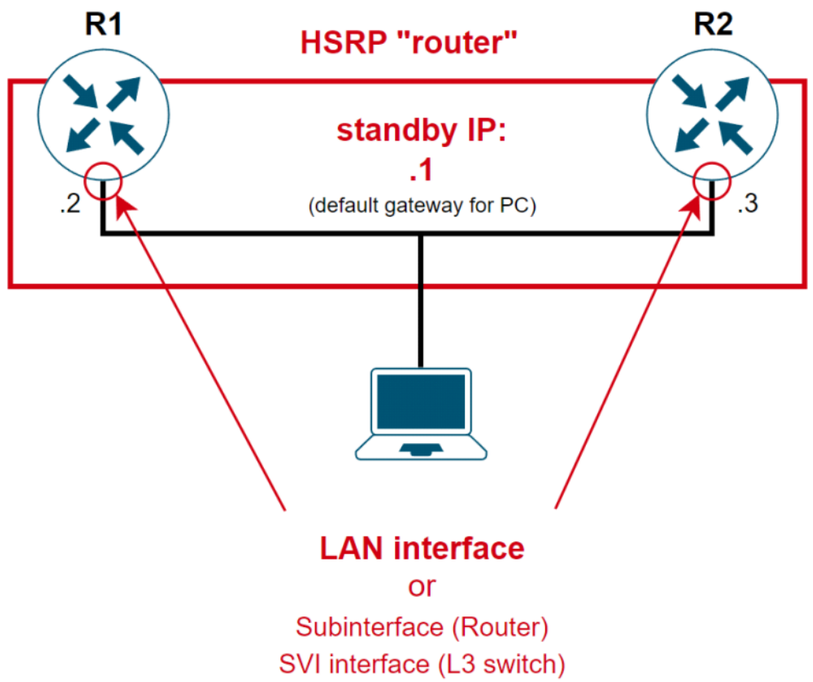
Thursday, 24 October 2024 10.22

```
!--------------------------------------
! HSRP
! ver 2 supports IPv6 (På Packet Tracer virker IPv6 HSRP ikke)
!
! IPv6 unicast-routing must be enabled on the device for
! HSRP IPv6 to be configured
!
! Default priority = 100 (Highest value best)
! Preempt gives the right to claim active role if you
! have higher priority
!--------------------------------------
```

R1	R2
ipv6 unicast-routing int <> ip address <> ipv6 address <> ipv6 address <fe80::2> link-local ! ! HSRP configuration standby version 2 standby 1 ip <> standby 1 priority <> standby 1 preempt standby 2 ipv6 autoconfig standby 2 priority <> standby 2 preempt	ipv6 unicast-routing int <> ip address <> ipv6 address <> ipv6 address <fe80::3> link-local ! ! HSRP configuration standby version 2 standby 1 ip <> standby 1 priority <> standby 1 preempt standby 2 ipv6 autoconfig standby 2 priority <> standby 2 preempt

```
sh standby [brief]
```

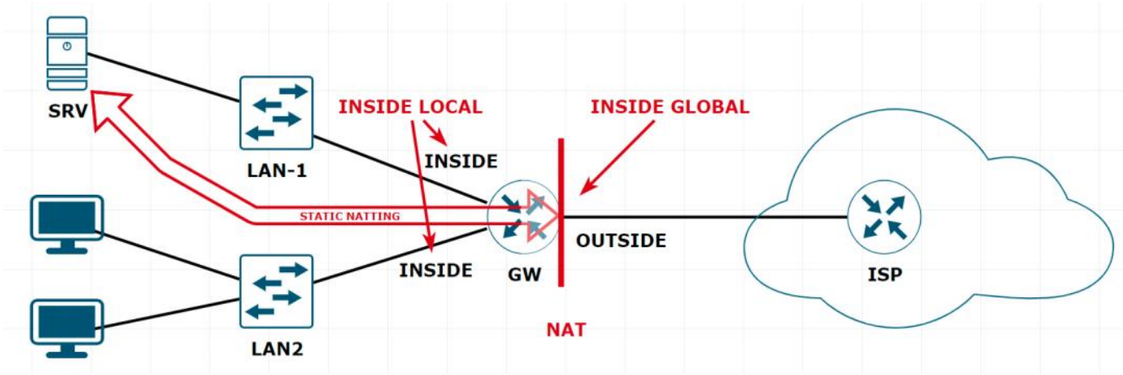
	IRDP (ICMP Router Discovery Protocol)	**HSRP** (Hot Standby Routing Protocol)	**VRRP** (Virtual Router Redundancy Protocol - IEEE standard)	**GLBP** (Gateway Load Balancing Protocol)
		1994	1999	2005
	Allows IPv4 hosts to locate routers that provide IPv4 connectivity to other (nonlocal) IP networks	Active-Standby	Master-Backup Master forward	AVG - Active Virtual Gateway AVF - Active Virtual Forwarder Primary-Secondary Round robin
RFC	RFC 1256	cisco proprietary RFC 2281	RFC 2338	cisco proprietary
Hello timer		3 sec	1 sec	3
Hold timer		10	3	
		0000.0c07.acxx (ver 1) 0000.0C9F.Fxxx (ver2)	0000.5e00.01xx	assigned by AVG 0007.b400.xxyy (up to four yy pr group xx)
			virtual IP or real IP	
		224.0.0.2 UDP 1985	224.0.0.18 UDP 112	224.0.0.102 UDP 3222
		preemption	preemption (default)	
		int track		int track
		Version 2 supports IPv6	Version 3 supports IPv6	



NAT

11. maj 2023 14:20

```
!------------------------------------------------------------
! Traditional NAT
! if port nat inside and NAT translation match in
! table -> route to outside int -> translate -> send
!------------------------------------------------------------
!
!------------------------------------------------------------
! Define WHERE to translate
!------------------------------------------------------------
int <outside-int>
 ip nat outside

int <inside-int>
 ip nat inside

!------------------------------------------------------------
! Define WHAT to translate
!------------------------------------------------------------
ip access-list standard <ACL-NAME> !(or use numbered ACL)
 remark Permit Local LAN to use NAT
 permit <source-net> <wm>

Do NOT use 'permit any'

!------------------------------------------------------------
! If needed switch standard ACL with extended ACL
!------------------------------------------------------------
ip access-list extended <ACL-NAME>
 remark Permit Local LAN to use NAT
 permit ip <LAN-net> <wm> any
 exit


!------------------------------------------------------------
! Define HOW to translate - PAT (mange til én)
!------------------------------------------------------------
ip nat inside source list <ACL-NAME> int <outside-int> overload

!------------------------------------------------------------
! Define HOW to translate - Dynamic NAT (mange til mange)
!------------------------------------------------------------
ip nat pool <Pool-NAME> <start-ip> <end-ip> prefix-length <>
ip nat inside source list <ACL-NAME> pool <POOL-NAME>

!------------------------------------------------------------
! Define HOW to translate - NAT with PAT
!------------------------------------------------------------
ip nat pool <Pool-NAME> <start-ip> <end-ip> prefix-length <>
ip nat inside source list <ACL-NAME> pool <POOL-NAME> overload

!------------------------------------------------------------
! Define HOW to translate - STATIC NAT
!------------------------------------------------------------
ip nat inside source static <inside-IP> <outside-IP>

!------------------------------------------------------------
! Define HOW to translate - STATIC NAT with PortForwarding
!------------------------------------------------------------
ip nat inside source static {tcp | udp} <local-ip local-port> <global-ip global-port>
```




```
!------------------------------------------------------------
! TROUBLESHOOTING:
!------------------------------------------------------------

sh ip nat statistics

sh ip nat translations
! if    * -> fast switched
! if no * -> process switched
! first packet is process-switched
! remaning packets go through fast switch path if a cache entry exists

debug ip nat [detailed]

clear ip nat translation *
clear ip nat statistics
```

Security - general

Thursday, 27 April 2023 10.55

```
!-----------------------------------------------
! Secure Management Access
!-----------------------------------------------
security passwords min-length 10
enable secret <pw>
service password-encryption
banner motd $Unauthorized access strictly prohibited!$

line con 0
 password <>
 exec-timeout <min> <sec>
 login
 logging synchronous
 exit
!
line vty 0 4
 password <>
 exec-timeout <> <>
 login
 logging synchronous
 exit
!
line aux 0
 no exec
```

Can you read the enable secret password?
No. The enable secret password is encrypted automatically using the MD5 or SHA hash algorithm. . IOS 15.0(1)S and later default to SHA256 hashing algorithm. SHA256 which is considered to be a very strong hashing algorithm and is extremely difficult to reverse. Earlier IOS versions use the weaker MD5 hashing algorithm.

```
!-------------------------------------
! security SSH
!-------------------------------------
hostname <>
ip domain-name <>
username <user> privilege 15 secret <pw>
!
line vty 0 4
 transport input ssh
 login local
 exit
!
crypto key generate rsa general-keys modulus 2048

ip ssh version 2
ip ssh time-out <sec>
ip ssh authentication-retries <>

! display version and configuration
sh ip ssh

! check the SSH connections to the device
sh ssh

ssh -l <username> <IP>
ssh -v <IP>
!-v = verbose (give more information)
ssh ?

! delete RSA key pair
crypto key zeroize rsa
```

```
!-------------------------------------
! security HTTP server (turn off if not in use)
!-------------------------------------
sh ip http server status
no ip http server

!-------------------------------------
! security Shutdown unused ports
!-------------------------------------
int range fa 0/x-y
 shutdown

!-------------------------------------
! Basic security:
!-------------------------------------
```

Blocks login attempts for 30 seconds if someone fails two attempts within 120 seconds

```
login block-for 30 attempts 2 within 120
sh login
```

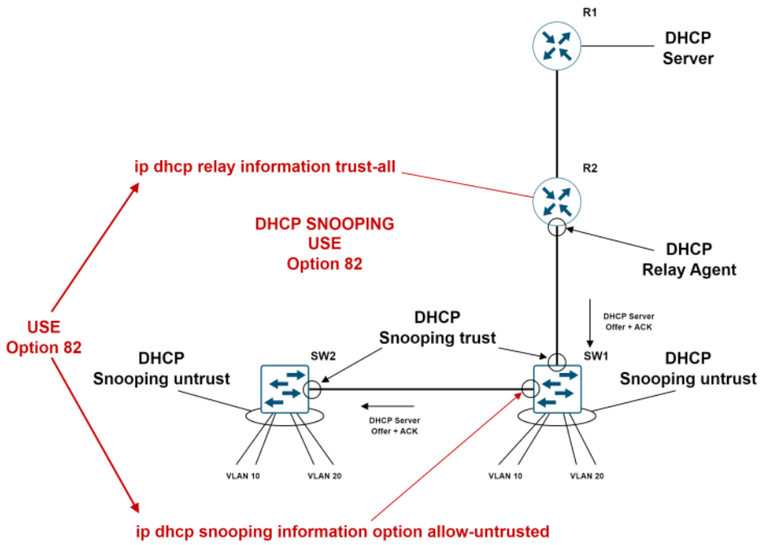
Security - switch

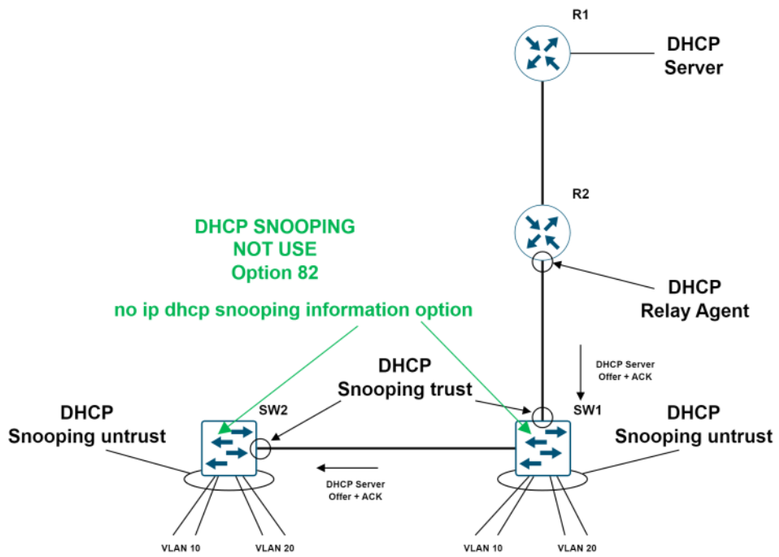
Thursday, 24 October 2024 12.55

```
!-------------------------------------------------------------
! Managing the MAC Address Table
!-------------------------------------------------------------
sh mac-address-table [dynamic]
sh mac-address-table <mac address>
clear mac-address-tabel [dynamic]

mac-address-table static <mac-address> vlan <vlan-id> int fa <>

int <>
 mac-address <>

!-------------------------------------------------------------
! Port Security
! Prevents i.e.:
! MAC address flooding and DHCP starvation attacks
!-------------------------------------------------------------
int fa 0/x
 switchport port-security ! this line turns on function
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security mac-address <mac-address>
 switchport port-security aging {static |time <> | type {absolute | inactivity}}
 switchport port-security violation {shutdown | restrict | protect}

sh port-security [address | int <>]

if port is in (err disabled)
 1. -> shutdown (administrativly shutdown)
 2. -> no shutdown
```

shutdown (default)	errdisable + log + snmp
restrict	drop + log + snmp
protect	drop

```
!-------------------------------------
! Secure unused ports
!-------------------------------------
int range fa0/X - Y
 shutdown
```






```
!-------------------------------------
! Packet Tracer doesn't fully support this
! DHCP Snooping (no lab)
! Prevents i.e.:
! DHCP starvation and DHCP spoofing attacks
!
! DAI (Dynamic Arp Inspection) (no lab)
! Prevents i.e.:
! ARP spoofing and ARP poisoning attacks
!-------------------------------------
ip dhcp snooping
no ip dhcp snooping information option
ip arp inspection validate [src-mac] [dst-mac] [ip]

! On all links where DHCP server packets are expected
int <>
 ip dhcp snooping trust
 ip arp inspection trust

! On all untrusted ports (optional)
int <>
 ip dhcp snooping limit rate <>

ip dhcp snooping vlan <>
ip arp inspection vlan <>
!


sh ip dhcp snooping
sh ip dhcp snooping binding
```

ACL (Access Control List)

Tuesday, 14 February 2023 09.36

```
!--------------------------------------------------------------------------
! Standard ACL (only look at source address)
! - place close to destination as default
!--------------------------------------------------------------------------
ip access-list standard <NAME>
 deny <NET> <WM> log
 permit any

int <int>
 ip access-group <NAME> {in|out}

!--------------------------------------------------------------------------
! Extended ACL (look at protocol, source-, dest-address and portno)
! - place close to source as default
!--------------------------------------------------------------------------
ip access-list extended <NAME>
 deny <protocol> <source-NET> <WM> <dest-NET> <WM> [eq <dest-port>] [log]
 permit ip any any

int <int>
 ip access-group <NAME> {in|out}

protocol  = ip, icmp, tcp...
host <IP> = <IP> 0.0.0.0
any       = 0.0.0.0 255.255.255.255

!--------------------------------------------------------------------------
! VTY ACL
!--------------------------------------------------------------------------
ip access-list standard VTY
 permit <NET> <WM>
 permit host <IP>
 deny any [log]

line vty 0 4
 access-class VTY in
!--------------------------------------------------------------------------
! ACL (numbered)
!--------------------------------------------------------------------------
!Standard access-list (1-99, 1300-1999)
access-list <1-99> permit/deny <IPno> WM

!Extended access-list (100-199, 2000-2699)
access-list <100-199> permit/deny <protocol> <sourceIP> WM <destIP> WM [eq portno]

interface ...
  ip access-group <no> in/out

sh access-lists
sh ip access-lists
sh ip int <int>
clear access-list counters
```

```
!-------------------------------------
! Well Known Port Numbers
!-------------------------------------
20-21 FTP
22    SSH
23    Telnet
25    SMTP
53    DNS
67/68 DHCP
80    HTTP
110   POP3
123   NTP
143   IMAP4
443   HTTPS
```

```
!-------------------------------------
! IPv6 ACL - now only extended named ACL
!-------------------------------------
The default bias template used by the Switch
Database Manager (SDM) does not provide IPv6
address capabilities. Verify that SDM is using
either the dual-ipv4-and-ipv6 template or the
lanbase-routing template. The new template will be
used after reboot even if the configuration is not
saved.

!-------------------------------------
! assign the dual-ipv4-and-ipv6
! template as the default SDM template
!-------------------------------------
sh sdm prefer
sdm prefer dual-ipv4-and-ipv6 default
reload

!-------------------------------------
! IPv6 ACL
!-------------------------------------
ipv6 access-list <NAME>
 permit…/x…
 deny…

int <>
 ipv6 traffic-filter <NAME> {in|out}

line vty 0 15
 ipv6 access-class <> in
```

Each IPv6 ACL contains *implicit* permit rules to enable IPv6 neighbor discovery.
These rules can be overridden by the user by placing a `deny ipv6 any any` statement at the end of the ACL. If, however, this statement is used, then the administrator must also specifically permit the neighbor discovery process as follows:

```
permit icmp any any nd-na
permit icmp any any nd-ns
deny ipv6 any any

!-------------------------------------
! reset match counters
!-------------------------------------
clear ipv6 access-list <NAME>

sh access-lists [NAME]

!-------------------------------------
! how to edit?
!-------------------------------------
remove from int
!insert new ACE
ipv6 access-list <NAME>
 permit…… sequence <no>
!append
 new ACE without sequence
!delete
 no ACE…
```

```
!-------------------------------------
! Bit Calculator
!-------------------------------------
```

	192	224	240	248	252	254	255
128	64	32	16	8	4	2	1

NTP, Syslog, SNMP

18. august 2023 14:27

```
!-------------------------------------------
! NTP
!-------------------------------------------
show clock
clock set <>

! NTP Server
ntp master <stratum-number>
! 0 = atomic clock
! 1 = attached to stratum 0 (also called ! 'timeservers')
! 2 = attached to stratum 1
!
! NTP Client
ntp server <NTP-server-ip>
ntp update-calendar ! update hardware calendar

sh ntp associations (~ configured, * peer, + candidate)
sh ntp status
debug ntp packet
```

```
!-------------------------------------------
! Syslog
!-------------------------------------------
service timestamps log datetime msec
logging host <Syslog-server-ip>
logging origin-id hostname
logging source-interface <>
logging trap <Severity Level>

sh logging

-------------------------------------------
logging origin-id ?
 hostname    Use origin hostname as ID
 ip          Use origin IP address as ID
 ipv6        Use origin IPv6 address as ID
 string      Define a unique text string as ID
 <cr>        <cr>
```

Syslog Severity Level

Severity Name	Severity Level	Explanation
Emergency **high**	Level 0	System Unusable
Alert	Level 1	Immediate Action Needed
Critical	Level 2	Critical Condition
Error	Level 3	Error Condition
Warning	Level 4	Warning Condition
Notification	Level 5	Normal, but Significant Condition
Informational	Level 6	Informational Message
Debugging **low**	Level 7	Debugging Message

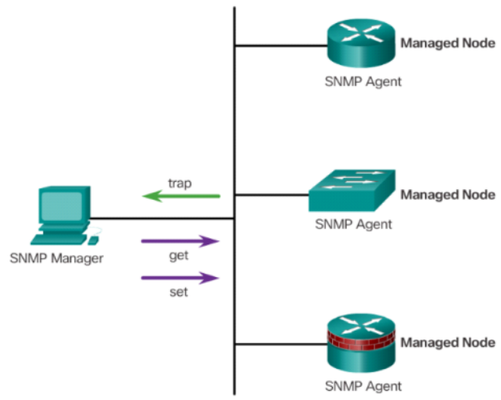
Syslog Message Format

Field	Explanation
seq no	Stamps log messages with a sequence number only if the `service sequence-numbers` global configuration command is configured.
timestamp	Date and time of the message or event, which appears only if the `service timestamps` global configuration command is configured.
facility	The facility to which the message refers.
severity	Single-digit code from 0 to 7 that is the severity of the message.
MNEMONIC	Text string that uniquely describes the message.
description	Text string containing detailed information about the event being reported.

```
seq no: timestamp: %facility-severity-MNEMONIC: description

00:00:46: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up
```

```
!-------------------------------------------
! SNMP (Simple Network Management Protocol)
! UDP port: 161/162
!-------------------------------------------
sh sdm prefer
sdm prefer lanbase-routing
reload

! Configure SNMP agent
snmp-server community ciscolab ro SNMP_ACL
snmp-server location snmp_manager
snmp-server contact ciscolab_admin
snmp-server host 192.168.1.3 version 2c ciscolab
snmp-server enable traps
ip access-list standard SNMP_ACL
 permit 192.168.1.3

sh snmp
sh snmp community
```

- **SNMPv1** - The Simple Network Management Protocol, a Full Internet Standard, defined in **RFC 1157**.
- **SNMPv2c** - Defined in **RFCs 1901 to 1908**; utilizes community-string-based Administrative Framework.
- **SNMPv3** - Interoperable standards-based protocol originally defined in **RFCs 2273 to 2275**; provides secure access to devices by authenticating and encrypting packets over the network. It includes these security features: **message integrity** to ensure that a packet was not tampered with in transit; **authentication** to determine that the message is from a valid source, and **encryption** to prevent the contents of a message from being read by an unauthorized source.



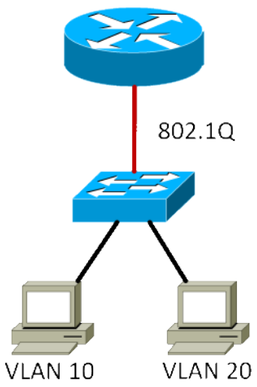
Operation	Description
`get-request`	Retrieves a value from a specific variable.
`get-next-request`	Retrieves a value from a variable within a table; the SNMP manager does not need to know the exact variable name. A sequential search is performed to find the needed variable from within a table.
`get-bulk-request`	Retrieves large blocks of data, such as multiple rows in a table, that would otherwise require the transmission of many small blocks of data. (Only works with SNMPv2 or later.)
`get-response`	Replies to a `get-request`, `get-next-request`, and `set-request` sent by an NMS.
`set-request`	Stores a value in a specific variable.

SNMPv1 and SNMPv2c Uses Community strings
SNMPv3 Adds Authentication and Encryption

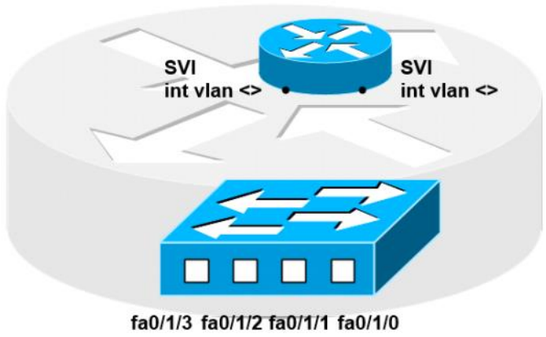
NMS (Network Management System)
- **SNMP Manager**
- **SNMP Agents**
  - **MIBs (Management Information Base)**

Inter-VLAN Routing

Monday, 22 August 2022 15.12




```
!--------------------------------------
! Inter-VLAN routing (router setup)
! Router-on-a-stick
!--------------------------------------
int fa 0/0
 no shutdown
!
int fa 0/0.<vlan-id>
 encapsulation dot1q <vlan-id> [native]
 ip address <IP> <SM>
```




```
!--------------------------------------
! Inter-VLAN routing
! (4 port switchmodul in router)
!--------------------------------------
ip routing

int vlan <x>
 description GW FOR VLAN X
 ip address <NET+SM>
!
int vlan <y>
 description GW FOR VLAN Y
 ip address <NET+SM>
!
int fa 0/1/0
 switchport mode access
 switchport access vlan <x>
!
int fa 0/1/1
 switchport mode access
 switchport access vlan <y>


sh vlan-switch
sh ip route
```

Static Routing

Saturday, 24 August 2024 14.25

```
!----------------------------------------
! Static Route
! adm distance: 1
!
!----------------------------------------
```

```
!-----------------------------------------------------
! Static IPv4 routes
!-----------------------------------------------------
ip route <network> <sm>  <exit-int> <next-hop-IP> [adm distance]
! in Packet Tracer choose only <next-hop-IP>
! on real equipment follow the syntax and use <exit-int> AND <next-hop-IP>

! default static route
ip route 0.0.0.0 0.0.0.0 <exit-int> <next-hop-IP>
```

```
!-----------------------------------------------------
! Static IPv6 routes
!-----------------------------------------------------
ipv6 route <ipv6-prefix/prefix-length> <exit-int> <next-hop-IP> [adm distance]

!default static route
ipv6 route ::/0 <exit-int> <next-hop-IP>
```

Static Route Types	Via …
Recursive Static Route or Next-Hop Static Route	Next-Hop-IP
Directly Connected Static Route	Exit interface
Fully Specified Static Route	Exit interface + Next-Hop-IP

Protocol	Administrative Distance
Connected	0
Static	1
EIGRP Summary Route	5
External BGP	20
EIGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
EGP	140
External EIGRP	170
Internal BGP	200
Unknown	255

RIP, RIPng, eBGP

Tuesday, 14 February 2023 09.37

```
!---------------------------------------
! RIP protocol
! adm distance: 120
! v1-255.255.255.255 v2-224.0.0.9
! UDP 520
! Algorithm: Bellman-Ford
! metric: hop (max 15 hop)
!---------------------------------------
router rip
 version 2
 no auto-summary
 passive-interface default
 no passive-interface <int>
 network <network>

!-------------------------------------
! to originate default route
! remember to make ip route 0.0.0.0/0
! often done on gateway router -> ISP
!-------------------------------------
 default-information originate
```

Note: Sometimes it is necessary to clear the RIP routing process before the default-information originate command will work.
First, try the command clear ip route * . Sometimes this does not work with RIP.
If still not working, save the configuration and then ***reload routers***. Doing this will reset the hardware and both routers will restart the RIP routing process.

```
sh ip protocols
sh ip route
sh ip rip database
clear ip route *
```

```
!---------------------------------------
! RIPng protocol
! adm distance: 120
! Multicast: FF02::9
! UDP 521
! Algorithm: Bellman-Ford
! metric: hop (max 15 hop)
!---------------------------------------
!
!-----------------------------------------------
! enable IPv6 routing
!-----------------------------------------------
ipv6 unicast-routing

!-----------------------------------------------
! enable rip on interface
!-----------------------------------------------
int <>
 ipv6 rip <process-name> enable

sh ipv6 protocols
sh ipv6 route
 - a RIPng router includes itself in the hop count
   ie. hop=2 is neighbour router
   a connected interface is 0 hop

!-----------------------------------------------
! passive-interface???
! There is NO passive-interface in RIPng
! - What to do? You have two options
! - 1) on the int you want to be passive - don't enable
!      RIPng - but use 'redistribute connected' under
!      the RIPng routing process.
! - 2) on the int you want to be passive - use a prefix-list
!      to filter all RIPng advertisements
!-----------------------------------------------


!-----------------------------------------------
! Originate default route
!-----------------------------------------------
! on interface pointing to internal network
! The originate keyword propagates the default route in addition
! to other routes in R2's routing table
int <>
 ipv6 rip <process-name> default-information {originate|only}

!-----------------------------------------------
! show commands
!-----------------------------------------------
sh ipv6 interface brief
clear ipv6 rip <process-name>
sh ipv6 protocols
sh ipv6 route rip
sh ipv6 rip
sh ipv6 rip database
sh ipv6 rip <process-name> next-hops
```

```
!---------------------------------------
! BGP protocol
! adm. distance: External = 20, Internal = 200
! TCP port 179
! Algorithm: Path Vector
!---------------------------------------
router bgp <as>
 bgp router-id <>
 neighbor <neighbor IP> remote-as <neighbor-as>
 network <> mask <subnet mask>

sh ip bgp
sh ip bgp summary
sh ip route
```

OSPFv2 (IPv4)

Tuesday, 14 February 2023 09.38

```
!-------------------------------------
! OSPF protocol
! adm distance: 110
! Multicast:
!  - 224.0.0.5 (all OSPF routers)
!  - 224.0.0.6 (all OSPF DRs)
! Algorithm: Dijkstra (SPF)
! Metric: cost (10^8/Bandwidth)
!-------------------------------------
router ospf <process-id>
 router-id <id in DDN>
 passive-interface {<> | default}
 network <net> <wm> area <area no>

 !-------------------------------------
 ! to originate default route
 ! remember to make ip route 0.0.0.0/0
 ! often done on gateway router -> ISP
 !-------------------------------------
 default-information originate [always]


sh ip protocols
sh ip ospf neighbor
sh ip ospf
sh ip ospf database
sh ip ospf interface
sh ip route

clear ip ospf <> process

!-------------------------------------
! link cost, hello and dead interval
!-------------------------------------
 ! increase the reference bandwidth
 ! to 10GigE
 ! default reference-bandwidth = 100Mb
 ! sh ip ospf
 auto-cost reference-bandwidth 10000

int s x/x
 bandwidth x (x in Kbits)
 ! cost = 10^8/BW
or
 ip ospf cost <value>

 ip ospf hello-interval <value>
 ip ospf dead-interval <value>
```

```
!-------------------------------------------------
! Summarize OSPF areas at the ABR
! (IPv4 and IPv6)
!-------------------------------------------------
router ospf <>
 area <> range <net> <sm>

sh ip route ospf

!-------------------------------------------------
! Summarize external routes into OSPF at the ASBR
! (IPv4 and IPv6)
!-------------------------------------------------
router ospf <pid>
 summary-address <net> <sm>

sh ip route ospf | include E2
```

```
!-------------------------------------
! How to reset Router-ID
!-------------------------------------
int lo0
 ip 1.1.1.1 255.255.255.255
reload
! or
router ospf 1
 router-id 1.1.1.1
clear ip ospf process
```

The **show ip ospf** command should be used to verify the OSPF router ID. If the OSPF router ID is using a 32-bit value other than the one specified by the **router-id** command, you can reset the router ID by using the **clear ip ospf** *pid* **process** command and re-verify using the command **show ip ospf**.

If an area is not connected to the backbone, its routes are not advertised outside of its area

```
!-------------------------------------------
! Activate interface for routing - new method
!-------------------------------------------
int <>
 ip ospf <> area <>
```

Note: Another option is to use the OSPF **network** command in router configuration mode.

Interface Type	10^8/bps = Cost
Fast Ethernet and faster	10^8/100,000,000 bps = 1
Ethernet	10^8/10,000,000 bps = 10
E1	10^8/2,048,000 bps = 48
T1	10^8/1,544,000 bps = 64
128 kbps	10^8/128,000 bps = 781
64 kbps	10^8/64,000 bps = 1562
56 kbps	10^8/56,000 bps = 1785

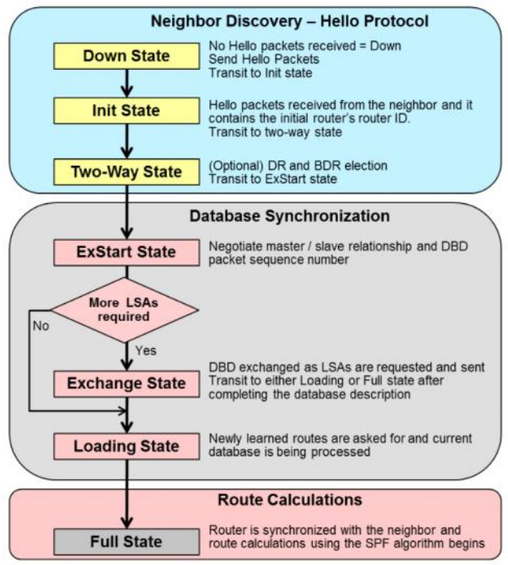

```
!-----------------------------
! OSPF Hello message
! * has to match!!
!-----------------------------
    -Router ID
    -Hello and Dead Timers*
    -Network mask*
    -Area ID*
    -Neighbors
    -Router priority
    -DR/BDR IP address
    -Authentication password*
    -Stub flag*
```

Type	Packet Name	Description
1	Hello	Discovers neighbors and builds adjacencies between them
2	Database Description (DBD)	Checks for database synchronization between routers
3	Link-State Request (LSR)	Requests specific link-state records from router to router
4	Link-State Update (LSU)	Sends specifically requested link-state records
5	Link-State Acknowledgment (LSAck)	Acknowledges the other packet types

```
type 1 - Router Link States (router ID)
type 2 - Net Link States (networks in area - intra area)
type 3 - Summary Net Link States (Inter Area)
type 4 - Summary ASB Link States (way to ASBR)
type 5 - Type-5 AS External Link States (external nets)
type 7 - Type-7 AS External Link States (external nets in NSSA)
```

```
!-------------------------------------
! show and debug commands
!-------------------------------------
sh ip ospf
sh ip ospf interface <>
sh ip ospf interface brief
sh ip route [ospf]
sh ip route static
sh run int <>

debug ip ospf ajd
clear ip ospf process
```

```
!-------------------------------------
! OSPF DR election on MultiAccess network
!
!-------------------------------------
!-------------------------------------
! link priority - default is 1
! 0 -> do not participate in DR election
! The one with highest value becomes DR
! - remember to clear ip ospf process
!-------------------------------------
int fa 0/0
 ip ospf priority <value>

If all have same link priority then:

DR = Highest Router-ID
priority:
  1) manuel router-ID
     router-id <>
  or
  2) automatic router-ID
     2a) Highest IP on loopback int
     2b) Highest IP on physical int
```




```
!-------------------------------------
! Make loopback int act as p2p in ospf
!-------------------------------------
```

Note: The default behavior of OSPF for loopback interfaces is to advertise a 32-bit host route. To ensure that the full /24 network is advertised, use the **ip ospf network point-to-point** command. Change the network type on the loopback interfaces so that they are advertised with the correct subnet.

```
int lo <>
 ip ospf network point-to-point
```

OSPFv3 (IPv6)

30. maj 2023 14:49

```
!-------------------------------------
! OSPFv3 protocol
! adm distance: 110
! Multicast:
!  - FF02::5 (all OSPF routers)
!  - FF02::6 (all OSPF DRs)
! Algorithm: Dijkstra (SPF)
! Metric: cost (10^8/Bandwidth)
!-------------------------------------
!
!-------------------------------------------------
! enable IPv6 routing
!-------------------------------------------------
ipv6 unicast-routing

sh run | section ipv6 unicast

!-------------------------------------------------
! enable OSPF routing on interface
!-------------------------------------------------
int <>
 ipv6 ospf <> area <>

!-------------------------------------------------
! Router-ID and other specific OSPFv3 cmd's
!-------------------------------------------------
ipv6 router ospf <process-id>
 router-id <n.n.n.n>
 passive-interface default
 no passive-interface <>
 default-information originate
```

Without any IPv4 addresses on the router, the OSPFv3 process will not start unless you manually set the router IDs.

```
! automatically generates a link-
! local address
ipv6 enable

!-------------------------------------
! IPv6 OSPF commands
!-------------------------------------
sh ipv6 protocols
sh ipv6 route …
sh ipv6 route ospf
sh ipv6 route static
sh ipv6 ospf
sh ipv6 ospf interface
sh ipv6 ospf database
sh ipv6 ospf neighbor
sh ipv6 interface
sh ipv6 int brief

clear ipv6 ospf <PID> process
```

```
Router Link States
Inter Area Prefix Link States
Link LSA (Type-8) Link States
Intra Area Prefix Link States
Type-5 AS External Link States
```

new types

- **Link LSA** (type 8)

Informs neighbors of link local address
Informs neighbors of IPv6 prefixes on link

- **Intra-Area Prefix LSA** (type 9)

Associates IPv6 prefixes with a network or router

	LSA Function Code	LSA type
Router-LSA	1	0x2001
Network-LSA	2	0x2002
Inter-Area-Prefix-LSA	3	0x2003
Inter-Area-Router-LSA	4	0x2004
AS-External-LSA	5	0x4005
Group-membership-LSA	6	0x2006
Type-7-LSA	7	0x2007
Link-LSA	8	0x0008
Intra-Area-Prefix-LSA	9	0x2009

EIGRP IPv4 - Classic Mode

11. maj 2023 10:17

```
!-------------------------------------------------
! EIGRP protocol
! Protocol: 88
! adm distance: Internal=90 - External=170 - Summary=5
! Multicast: 224.0.0.10 or MAC address 01:00:5e:00:00:0a
! Algorithm: DUAL (Diffused Update Algorithm)
! metric: BW+DLY (default)
!-------------------------------------------------
router eigrp <AS>
 eigrp router-id <>
 no auto-summary
 passive-interface {<> | default}
 no passive-interface <int>
 network <net> [<WM>]

!-------------------------------------
! to originate default route
! remember to make ip route 0.0.0.0/0
! often done on gateway router -> ISP
!-------------------------------------
 redistribute static

!-------------------------------------
! Bandwidth
!-------------------------------------
int S x/x
 bandwidth <Kbits>
 ip bandwidth-percent eigrp <AS> <percent>

 !-------------------------------------
 ! Manual summarization
 !-------------------------------------
 ip summary-address eigrp <AS> <NET+SM>

 !-------------------------------------
 ! Manipulate EIGRP timers
 !-------------------------------------
 ip hello-interval eigrp <AS> <SEC> ! default 5 sec
 ip hold-time eigrp <AS> <SEC>      ! default 3x hello

! Show commands
sh ip protocols
sh ip route [<net> <sm>]
sh ip route summary
sh ip route eigrp
sh ip eigrp neighbors
sh ip eigrp interfaces [detail]
sh ip eigrp topology [<prefix>] [all-links]
sh protocols
sh int <>
sh interfaces description

debug eigrp packets
debug ip eigrp <AS>
debug ip eigrp summary
```

```
!-------------------------------------------------
! Load balancing
!-------------------------------------------------
!-------------------------------------------------
! disable cef and route caching
! -> per-packet load balancing
! enable cef and route caching
! -> per-destination load balancing
!-------------------------------------------------
no ip cef
int <>
 no ip route-cache

debug ip packet
```

Another way to demonstrate per-packet load balancing, that does not disable CEF, is to use the per-packet load balancing command **ip load-share per-packet** on outgoing interfaces S0/0/0 and S0/0/1

```
!-------------------------------------------------
! enable unequal load balancing
! variance 2 command, which allows unequal-cost load
! balancing bounded by a maximum distance of (2) × (FD)
!-------------------------------------------------
router eigrp <as>
 variance <>
 maximum-path <> !default =4

sh ip route <net>
!look for traffic share count (0=not in use)

sh ip protocols
!look for 'maximum path' and 'maximum metric variance'
```

Advertised Distance/Reported Distance (AD or RD)
- the metric for an EIGRP neighbour router to reach the destination; the metric between the next-hop router and the destination

Feasible Distance (FD=local cost + AD)
- the sum of the AD from the next-hop neighbour, and the cost between the local router and the next-hop router

Successor (lowest FD)
Feasible successor (FS has an AD < current Successor)
Passive Versus **Active** Routes
- Passive is the operational, stable state
- A route is active when it is undergoing recomputation

```
!-------------------------------------------------
! EIGRP Stub
!-------------------------------------------------
Routers configured as stubs do not forward EIGRP learned routes to
other neighbors.
Use the eigrp stub command to configure a router as a stub where the
router directs all IP traffic to a distribution router.

router eigrp <as>
 eigrp stub <> !default connected and summary

  connected      Do advertise connected routes
  leak-map       Allow dynamic prefixes based on the leak-map
  receive-only   Set receive only neighbor
  redistributed  Do advertise redistributed routes
  static         Do advertise static routes
  summary        Do advertise summary routes

  receive-only works only alone
  usage: ie on router with NAT/PAT

sh run | sec eigrp
sh ip eigrp neighbors detail
```

EIGRP IPv6 - Classic Mode

11. maj 2023 10:36

```
!-------------------------------------------------
! EIGRP for IPv6 protocol
! adm distance: Internal=90 - External=170 - Summary=5
! Multicast: FF02::A
! Algorithm: DUAL (Diffused Update Algorithm)
! metric: BW+DLY (default)
!-------------------------------------------------
!
!-------------------------------------------------
! enable IPv6 routing
!-------------------------------------------------
ipv6 unicast-routing

!-------------------------------------------------
! enable EIGRP routing on interface
!-------------------------------------------------
int <>
 ipv6 eigrp <as>
```

The interfaces can be directly configured with EIGRP for IPv6, without the use of a global IPv6 address. There is no network statement in EIGRP for IPv6.

```
!-------------------------------------------------
! Router-ID and other specific EIGRPv6 cmd's
!-------------------------------------------------
ipv6 router eigrp <as>
 eigrp router-id <>
 passive-interface default
 no passive-interface <>
 [no shutdown] !default from IOS 15.2
```

Without any IPv4 addresses on the router, the EIGRPv6 process will not start unless you manually set the router IDs.

EIGRP for IPv6 has a shutdown feature. Ensure that the routing process is in "no shut" mode in order to run the protocol.

```
!-------------------------------------------------
! manual summarisation
!-------------------------------------------------
int <>
 ipv6 summary-address eigrp <as> <net/x>

sh ipv6 route eigrp

!-------------------------------------------------
! default route
!-------------------------------------------------
ipv6 route ::/0 <exit-int> <next-hop-ip>

ipv6 router eigrp <as>
 redistribute static
```

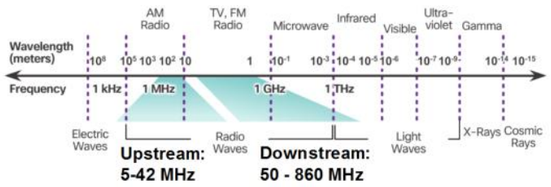
Note: With the use of CEF (Cisco Express Forwarding) it is recommended practice that a next-hop IP address is used instead of an exit-interface. There is a bug in IOS 15.4 that prevents an IPv6 static route with only a next-hop address from being redistributed. A fully specified static route with both an exit-interface and a next-hop address is used in the example.

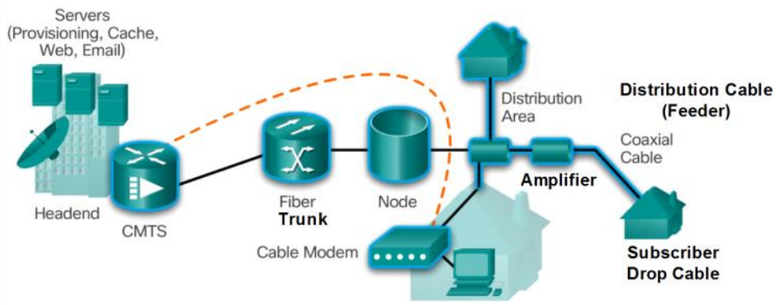
```
!-------------------------------------------------
! enable IPv6 cef
!-------------------------------------------------
ipv6 cef

sh ipv6 cef [summary]

sh ipv6 eigrp neighbors
sh ipv6 route eigrp
sh ipv6 eigrp topology
sh ipv6 protocols
```

Broadband Systems

Tuesday, 14 February 2023 09.45

Cable System: (SHARED)





DOCSIS: Data Over Cable Service Interface Specification
- OSI Layer 1 & 2
- L1/Physical layer: Channel widths (Bandwidths) pr. channel, Modulation Technique
- L2/MAC layer: Defines a deterministic **access method**
  - TDMA (Time-Division Multiple Access)
  - FDMA (Frequency-Division Multiple Access)
  - S-CDMA (Synchronous Code Division Multiple Access)

Access Method Analogy:
Room full of people asking for "Channel Access" speak time
- Speak in turn (Time Division)
- Speak in different pitch (Frequency Division)
- Speak in different languages (Code Division)

CMTS (Cable Modem Termination System)
- A cable modem termination system (CMTS) is a component that exchanges digital signals with cable modems on a cable network. A headend CMTS communicates with CMs that are located in subscriber homes.

CM (Cable Modem)
- A cable modem enables you to receive data at high speeds. Typically, the cable modem attaches to a standard 10BASE-T Ethernet card in the computer.

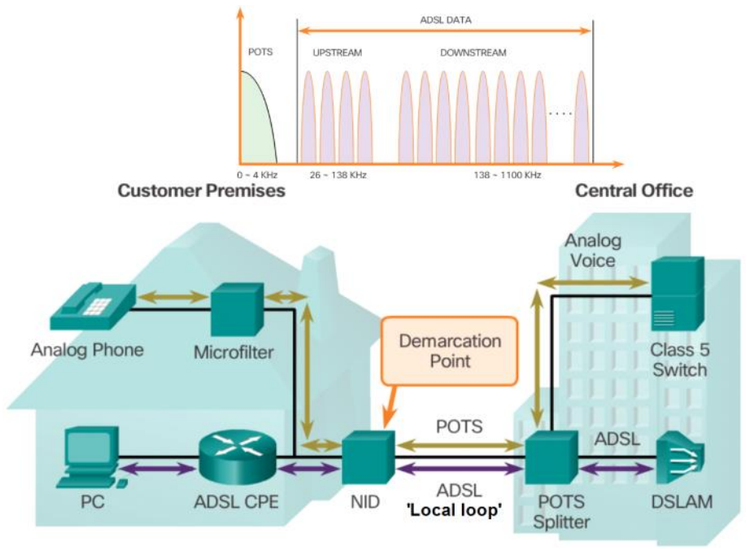
Fiber
- The trunk portion of the cable network is usually fiber optic cable.

Node
- Nodes convert optical signals to RF signals.

In a modern HFC network,
typically 500 to 2,000 active data subscribers are connected to a cable network segment, all sharing the upstream and downstream bandwidth.
The actual bandwidth for Internet service over a CATV line can be **up to 160 Mb/s downstream** with the latest iteration of DOCSIS, and **up to 120 Mb/s upstream**.

More speed needed?
- Allocate more Bandwidth from TV channels
- Subdevide User Segments

DSL (Digital Subscriber Line)



Delivered over telephone Cable
- 300 Hz - 3 KHz - telephony
- 3 KHz - 1 MHz - DSL

ADSL (Asymmetric DSL) 20 KHz - 1 MHz
- Downstream Bandwidth higher
- Upstream Bandwidth lower

SDSL (Symmetric DSL)
- Downstream/Upstream Bandwidth = same

Bandwidth depend on '**local loop**'
- Local loop max 5.46 km
- > 40 Mbps

DSLAM (DSL Access Multiplexer)
CO (Central Office)
CPE (Customer Premises Equipment)

Transceiver
- Connects the computer of the teleworker to the DSL. Usually the transceiver is a DSL modem connected to the computer using a USB or Ethernet cable. Newer DSL transceivers can be built into small routers with multiple 10/100 switch ports suitable for home office use

DSLAM
- Located at the CO of the carrier, the DSLAM combines individual DSL connections from users into one high-capacity link to an ISP, and therefore, to the Internet

Filters:
NID (Network Interface Device) - POP (Point Of Precense)
Splitter: Low-pass filter (0-4KHz)
Microfilter: (two ends)

Wireless Broadband technologies

WLAN/Wi-Fi IEEE 802.11 - up to 7Gbps
Hotspot is an area covered by one og more interconnected Access Points (AP)

Minicipal Wi-Fi - mesh topology
- Bynet
- Police
- Fire Fighters
- City workers

WiMAX IEEE 802.16 (Worldwide Interoperability for Microwave Access)
- Point to Multipoint
- Wireless celluar
- Up to 1Gbps
- (danmark - Skyline, Butler Networks, Danske Telecom…)

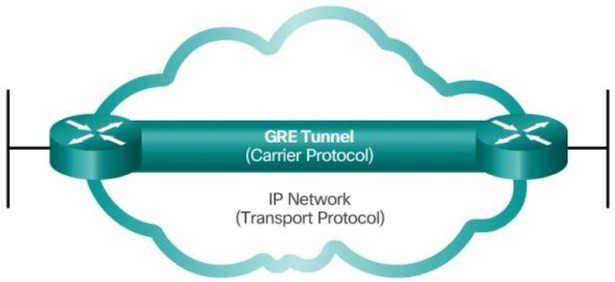
A WiMAX network consists of two main components:
- **A towe**r that is similar in concept to a cellular telephone tower. A single WiMAX tower can provide coverage to an area as large as 3,000 square miles (**7,500 square km**).
  A WiMAX tower station connects directly to the Internet using a high-bandwidth connection, such as a T3 line. A tower can also connect to other WiMAX towers using line-of-sight microwave links. WiMAX is thus able to provide coverage to rural areas out of reach of last mile cable and DSL technologies
  - Bit rate is limited to 2 Mb/s per subscriber, cell size is 1 to 2 km (1.25 mi).
- **A WiMAX receiver** that is connected to a USB port or is built into a laptop or other wireless device.

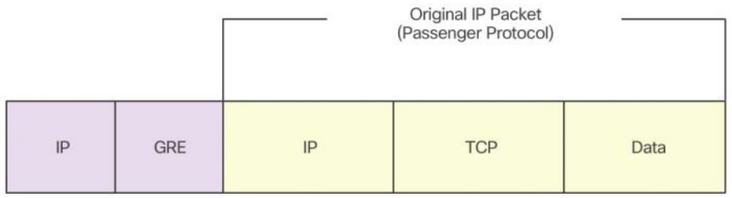
Mobile broadband
- 2G (GSM, CDMA, TDMA)
- 3G (UMTS, CDMA2000, EDGE, HSPA+)
- 4G (WiMAX, LTE)
  - LTE (Long-Term Evolution)

Satelite Internet
- Up to 10Mbps
- Vessels at sea
- Airplanes in flight
- Vehicles moving on land
- VSAT (Very Small Aperture Terminals) used for private WAN
- **One-way multicast** - Satellite Internet systems are used for **IP multicast-based data, audio, and video distribution**. Even though most IP protocols require two-way communication for Internet content including web pages, one-way satellite-based Internet services can be used to push pages to local storage at end-user sites. Two-way interactivity is impossible.
- **One-way terrestrial return** - Satellite Internet systems use **traditional dialup access** to send outbound data through a modem and receive downloads from the satellite.
- **Two-way satellite Internet** - **Sends data from remote sites via satellite to a hub, which then sends the data to the Internet**. The satellite dish at each location needs precise positioning to avoid interference with other satellites.
  Can serve up to 5.000 communication channels simultaneously.

VPNs (GRE, IPsec)

Tuesday, 14 February 2023 09.45





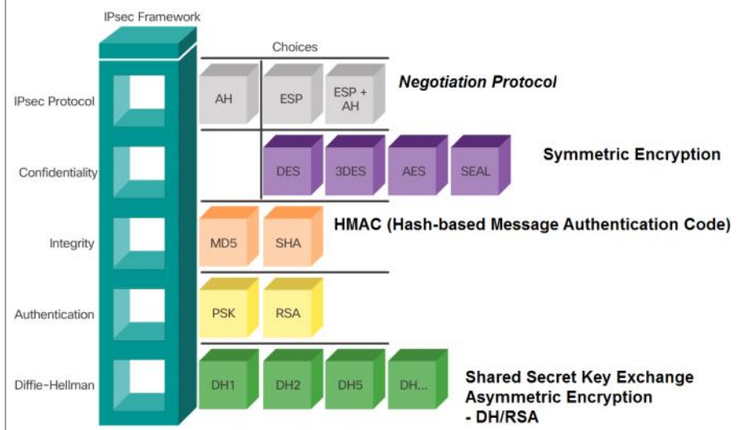

```
!--------------------------------------------
! Point-to-Point GRE VPN Tunnel
! GRE (Generic Routing Encapsulation)
! Protocol: 47
! Adds min 24 bytes extra header
!--------------------------------------------
int tunnel 0
 ip address <>
 ! tunnel mode <encapsulating protocol> <transport protocol>
 ! tunnel mode gre ip ! This is default
 tunnel source <local-int>
 tunnel destination <remote-ip>
!
sh ip int brief
sh int tunnel <>
```

```
!--------------------------------------------
! IPsec
!--------------------------------------------
```

IETF standard that defines how a VPN can be configured in a secure manner using the internet Protocol
IPsec is a framework of open standards that spells out the rules for secure communications

IPsec characteristics can be summarized as follows:

- IPsec is a framework of open standards that is algorithm-independent.
- IPsec provides data confidentiality, data integrity, and origin authentication.
- IPsec acts at the network layer, protecting and authenticating IP packets.



Symmetric Encryption:

- use same key to encrypt and decrypt data

Asymmetric Encryption:

- use one key to encrypt and another key to decrypt
- Public/Private key

IPsec framework protocol

- When configuring an IPsec gateway to provide security services, an IPsec protocol must be selected. The choices are some combination of ESP and AH. Realistically, the **ESP or ESP+AH** options are almost always selected because AH itself does not provide encryption.
  - AH (authentication Header)
    - Authentication
    - Integrity
  - ESP (Encapsulating Security Payload)
    - Encryption
    - Authentication
    - Integrity

Confidentiality (encryption)

- (If IPsec is implemented with ESP) - The encryption algorithm chosen should best meet the desired level of security: DES, 3DES, or AES. AES is strongly recommended, with AES-GCM providing the greatest security.

Integrity (Original Data)

- Guarantees that the content has not been altered in transit. Implemented through the use of hash algorithms. Choices include MD5 and SHA.

Integrity with Hash Algorithms

HMAC (Hash-based Message Authentication Code)

VPNs use a message authentication code to verify the integrity and the authenticity of a message, without using any additional mechanisms.

There are two common HMAC algorithms:

MD5 - Uses a 128-bit shared secret key. The variable-length message and 128-bit shared secret key are combined and run through the HMAC-MD5 hash algorithm. The output is a 128-bit hash. The hash is appended to the original message and forwarded to the remote end.

SHA - SHA-1 uses a 160-bit secret key. The variable-length message and the 160-bit shared secret key are combined and run through the HMAC-SHA1 hash algorithm. The output is a 160-bit hash. The hash is appended to the original message and forwarded to the remote end.

Authentication (Source Authentic)

- Represents how devices on either end of the VPN tunnel are authenticated. The two methods are PSK or RSA.

There are two peer authentication methods:

PSK - A secret key that is shared between the two parties using a secure channel before it needs to be used. Pre-shared keys (PSKs) use symmetric key cryptographic algorithms. A PSK is entered into each peer manually and is used to authenticate the peer. At each end, the PSK is combined with other information to form the authentication key.

RSA signatures - Digital certificates are exchanged to authenticate peers. The local device derives a hash and encrypts it with its private key. The encrypted hash, or digital signature, is attached to the message and forwarded to the remote end. At the remote end, the encrypted hash is decrypted using the public key of the local end. If the decrypted hash matches the recomputed hash, the signature is genuine.

DH algorithm group

- Represents how a shared secret key is established between peers. There are several options, but DH24 provides the greatest security.

ISAKMP Framework (Internet Security Association and Key Management Protocol)

IKE protocol (Internet Key Exchange)

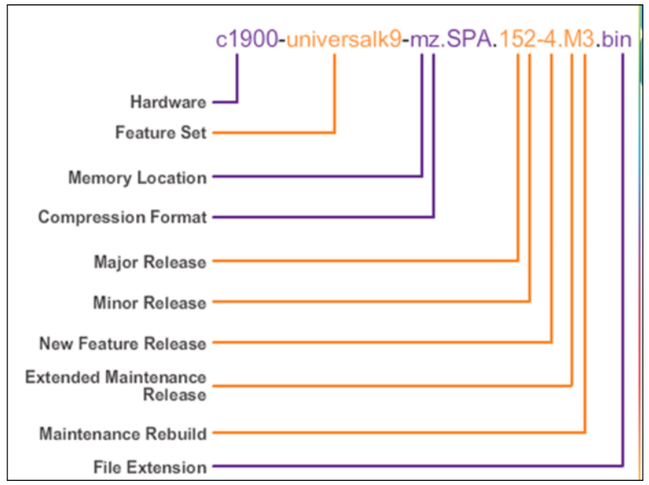
DH (Diffie-Hellman Key Exchange) - PKE (Public Key Exchange method)

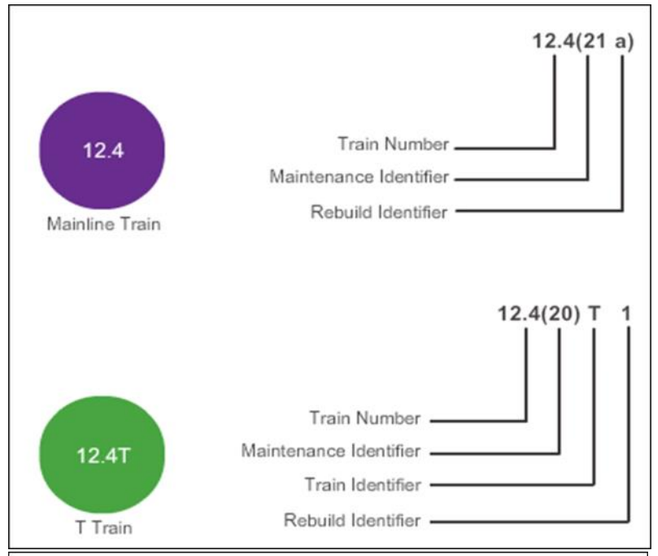
- a method to securely exchange the keys that encrypt data. (DH) algorithms allow two parties to establish a shared secret key that is used by encryption and hash algorithms.
- The DH algorithm specifies a public key exchange method that provides a way for two peers to establish a shared secret key that only they know, although they are communicating over an insecure channel. Like all cryptographic algorithms, DH key exchange is based on a mathematical sequence of steps.

IOS

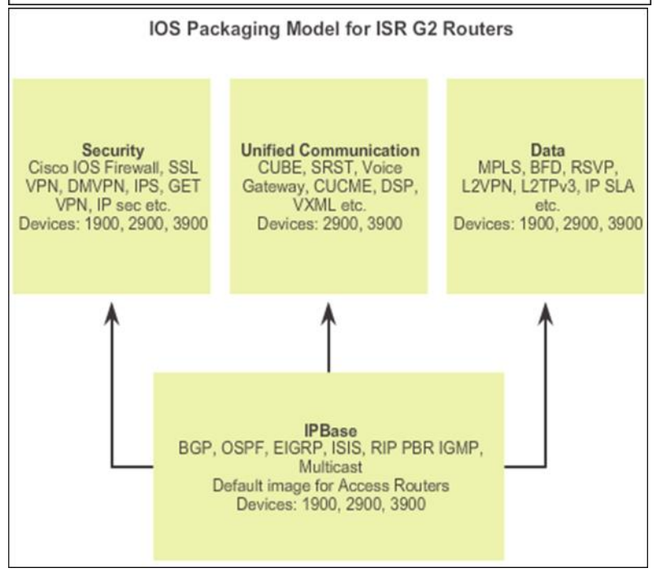
Tuesday, 14 February 2023 09.44

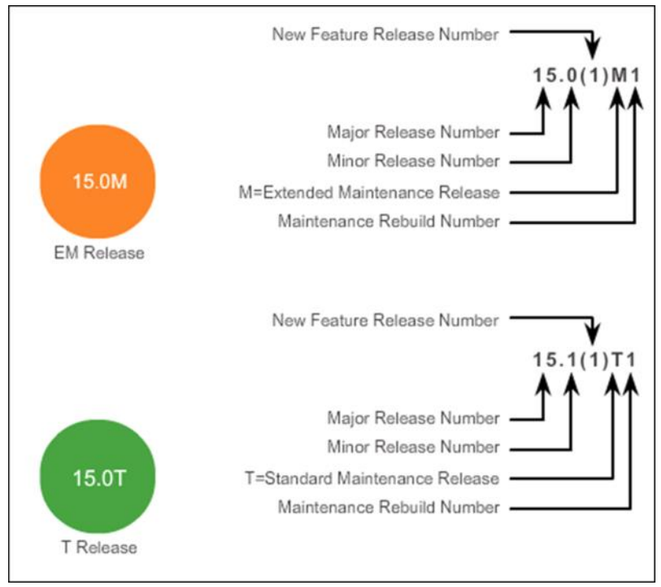
```
!--------------------------------------------
!Manage IOS and Configs
!--------------------------------------------
show version
show flash:
rename flash:/… flash:/
dir flash:
delete flash:/…/html/*

archive tar /x tftp://<ip-of-tftp>/<ios-name> flash:/<dir>

copy <source [flash:|tftp:|ftp:]> <destination [flash:|tftp:|ftp:]>
copy startup-config tftp:
erase nvram
copy tftp: startup-config

cd flash:/<dir>

config t
boot system flash://c1900-universalk9-mz.SPA.152-4.M3.bin
boot system tftp://c1900-universalk9-mz.SPA.152-4.M3.bin
boot system rom

show boot
```






```
!--------------------------------------------
!IOS license handling
!--------------------------------------------

show version
show license [udi]

config t
 license install <stored-location-url>
 license accept end user agreement ------- accept EULA
 license boot module c1900 technology-package [datak9|ipbasek9|securityk9]
 end
write
reload

license save flash::all-licenses.lic

copy <source> <destination>
config t
 boot system flash://c1900-universalk9-mz.SPA.152-4.M3.bin
 boot system tftp://c1900-universalk9-mz.SPA.152-4.M3.bin
 boot system rom

Remove licenses:
config t
 license boot module c1900 technology-package [datak9|ipbasek9|securityk9] disable
 end
reload
license clear [datak9|ipbasek9|securityk9]
config t
 no license boot module c1900 technology-package [datak9|ipbasek9|securityk9]
 end
reload
```

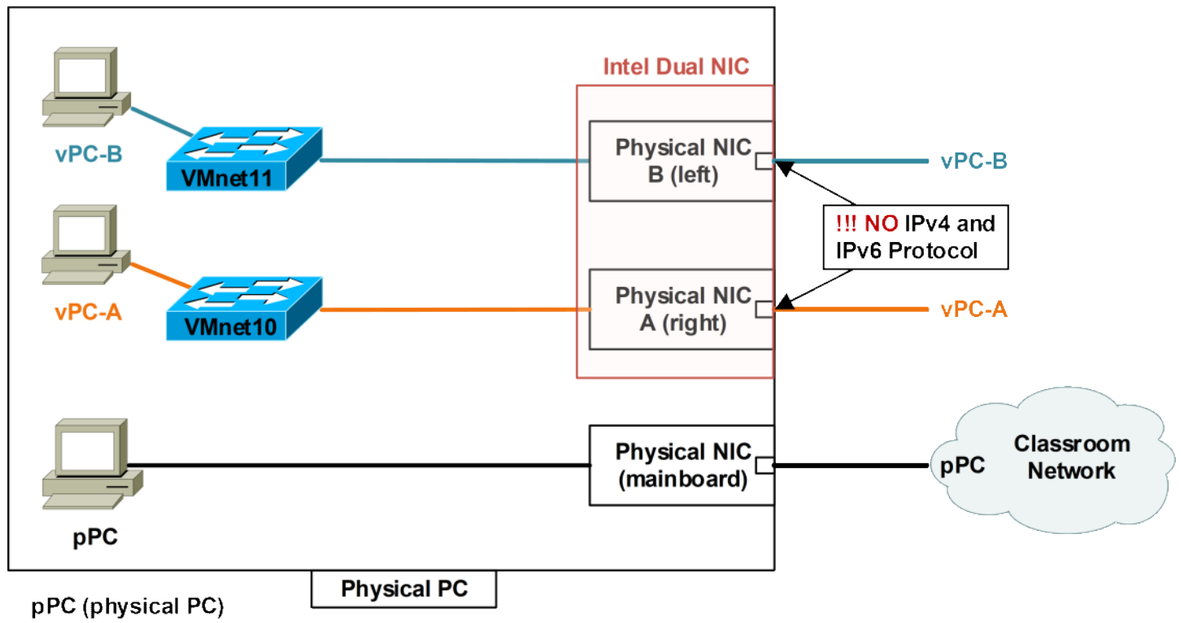




Virtual PC's - how to connect to LABs

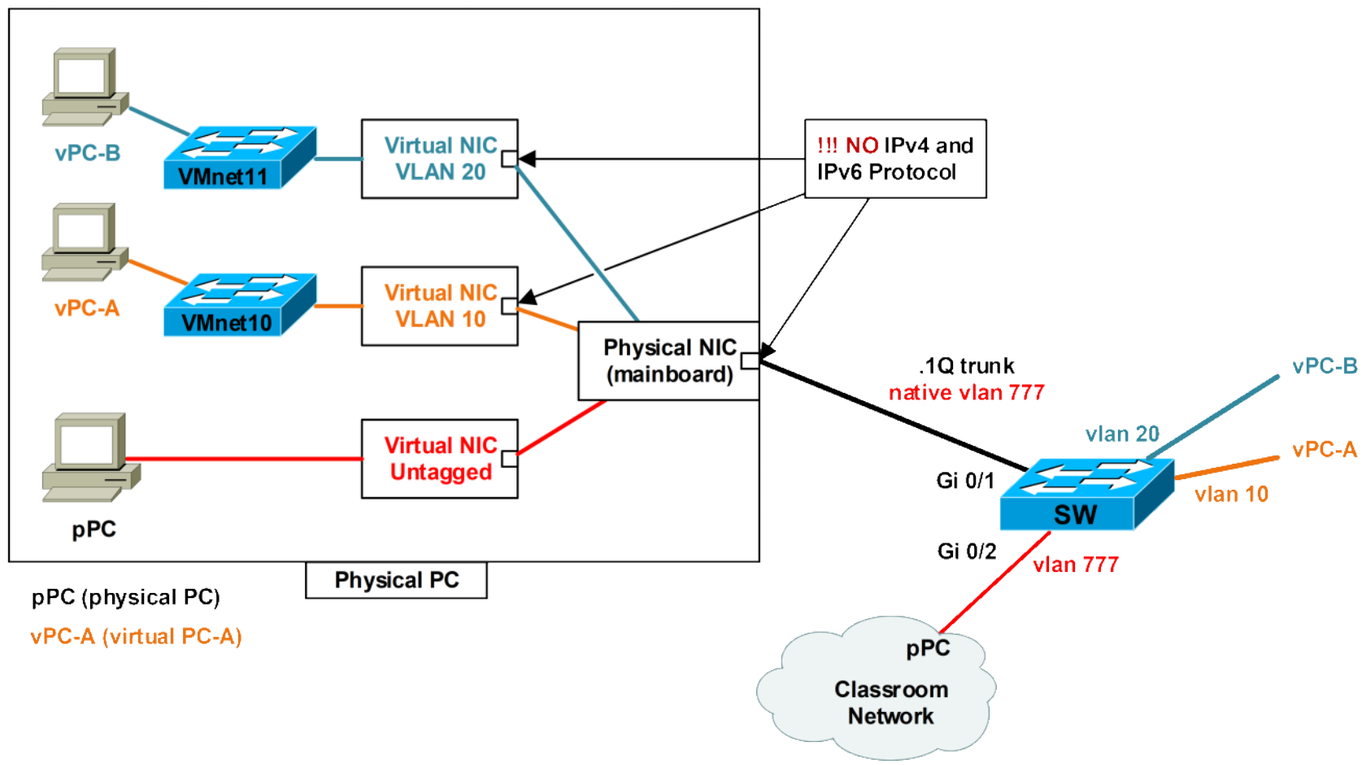
Tuesday, 14 February 2023 09.46

Every virtual PC to using separate physical NIC
Physical PC always connected to Internet (Classroom Network)



pPC (physical PC)
vPC-A (virtual PC-A)

Virtual PCs and Physical PC via one physical NIC to Switch, using dot1Q trunk.
Physical PC always connected to Internet (Classroom Network)



pPC (physical PC)
vPC-A (virtual PC-A)