<3G Networks>

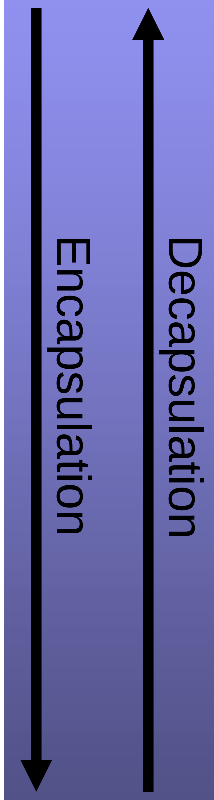
Intro to Networking
Mikrotik/Cisco

Terms Used

- Layer X – When I refer to something being at layer X I’m referring to the OSI model.
- VLAN – 802.1Q Layer 2 marking on traffic used to segment sets of traffic. VLAN tags are applied on access ports.
- Trunk – I’m referring to an 802.1Q trunk port. This is a method to transmit frames across an L2 link with a VLAN tag intact.
- Outside/Inside – Outside refers to the interface connecting you to the Internet where as Inside refers to the interface connecting you to the LAN side of your router. I’ll use these terms most often when talking about NAT.

- NAT/PAT – Network Address Translation. This take a private address (RFC1918) and translates it to a publically routable IP. Port Address Translation is a method to translate multiple private addresses to a single public IP (masquerade).
- DHCP – Dynamic Host Configuration Protocol – Auto assign IP on hosts. TCP port 67.
- NTP – Network Time Protocol. Synchronizes your system time to an external time server.
- Bridging – Refers to layer 2 connectivity between multiple ports.

OSI Model - 7 Layers



Encapsulation

Decapsulation

- 7 – Application – Interact directly with Apps (FTP, HTTP, SMTP)
- 6 – Presentation – Formats data (encryption)
- 5 – Session – Controls connections between computers
- 4 – Transport – TCP/UDP – ports - Segment
- 3 – Network – IP addressing - Packet
- 2 – Data Link – MAC addressing - Frame
- 1 – Physical - Electricity

L7 - Application

- HTTP.
- SNMP.
- SMTP.
- Interacts directly with your applications.

L6 - Presentation

- Encoding.
- Encryption.

L5 - Session

- Manages connections between local and remote applications.
- Not usually used in the IP suite.

L4 – Transport

- TCP/UDP live here.
- Connection and connectionless oriented traffic.
- Use ports to keep track of conversations.
- PDU at this level is a Segment.

TCP

- Connection oriented – reliable.
- FTP, SMTP, HTTP.
- Flow control – how much traffic can the receiving end handle.
- Window size – how many packets can be received before an acknowledgement (ACK) must be sent.
- 3-way handshake –
  - SYN =>
  - SYN + ACK <=
  - ACK =>
  - *We are now established*

UDP

- Connection less – best effort.
- TFTP, RTP.

TCP vs UDP

- Sequenced - Unsequenced
- Reliable - Unreliable
- Connection-oriented - Connectionless
- Virtual Circuit - Low overhead
- Acks - No Acks
- windowing/flow control - None

L3 - Network

- IP addressing.
- Connects LAN segments.
- Protocol numbers are L3 facilities.
- PDU at this level is Packet.

Protocols

- 1 - ICMP
- 6 - TCP
- 17 - UDP
- 47 - GRE
- 50 - ESP
- 51 - AH
- 112 - VRRP
- 115 - L2TP
- Don't confuse UDP/TCP ports with protocol numbers.

L2 – Data Link

- MAC addressing – Media Access Control.
- ARP – Address Resolution Protocol operates at this level. This is an IP to MAC lookup process. Though L3 uses this, ARP has no protocol number.

L1 - Physical

- Where our frame is transferred to electricity and sent across a wire.
- Covers cabling types.
- This is as high as hubs go in the OSI model.

Switch Vs Hub

- Layer 2 – Layer 1.
- Full Duplex (4 wires) – Half duplex (2 wires).
- Every port single collision domain – 1 big collision domain *both have single broadcast domain*.
- Not needed – CSMA/CD (Carrier Sense Multi Access.
- Switch good – Hub bad.

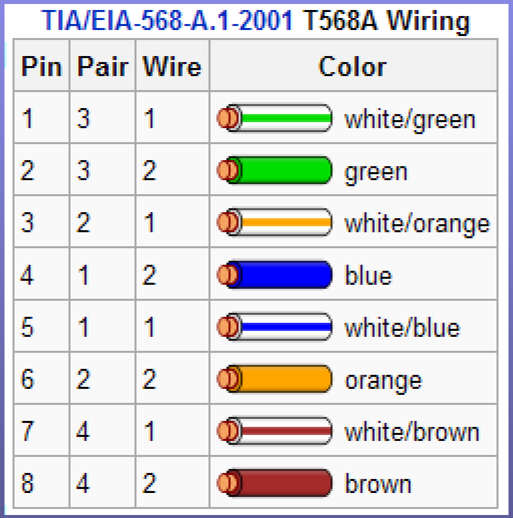
Bridging/Switching

- Bridges were introduced to connect LAN segments in hub environments. They were generally 2 port guys. Software based devices. Broke the hub network’s collision domains up.
- Switches came along which are pretty much multi port bridges.
- Bridges are usually implemented in software where as switches are generally hardware based devices. Switches include ASICs (Application Specific Integrated Circuits) that do the switching.
- In Mikrotik when you create a bridge interface and add ports, this is all done in software, which is why the CPU takes a performance hit in heavy bridging operations. Some models like the RB450s and the RB750 have some switching ASICs which is why you get wire speed performance when using this ports configured properly.
- Cisco has been ASIC based since they bought the Catalyist series switches.

Cabling

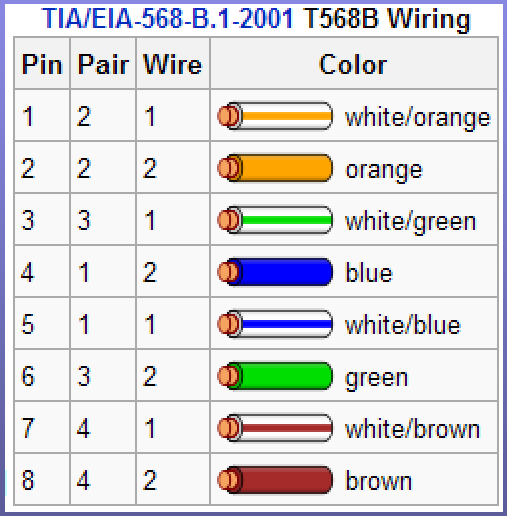
- Straight through – Host to Switch.
- Cross over – Switch to Switch or Host to Host.
- Hosts are routers and PCs.
- MDI/MDI-X is sometimes employed which is an “auto crossover” technology. It senses whether or not the cable needs to be crossed.

Type A or B Standard



TIA/EIA-568-A.1-2001 T568A Wiring

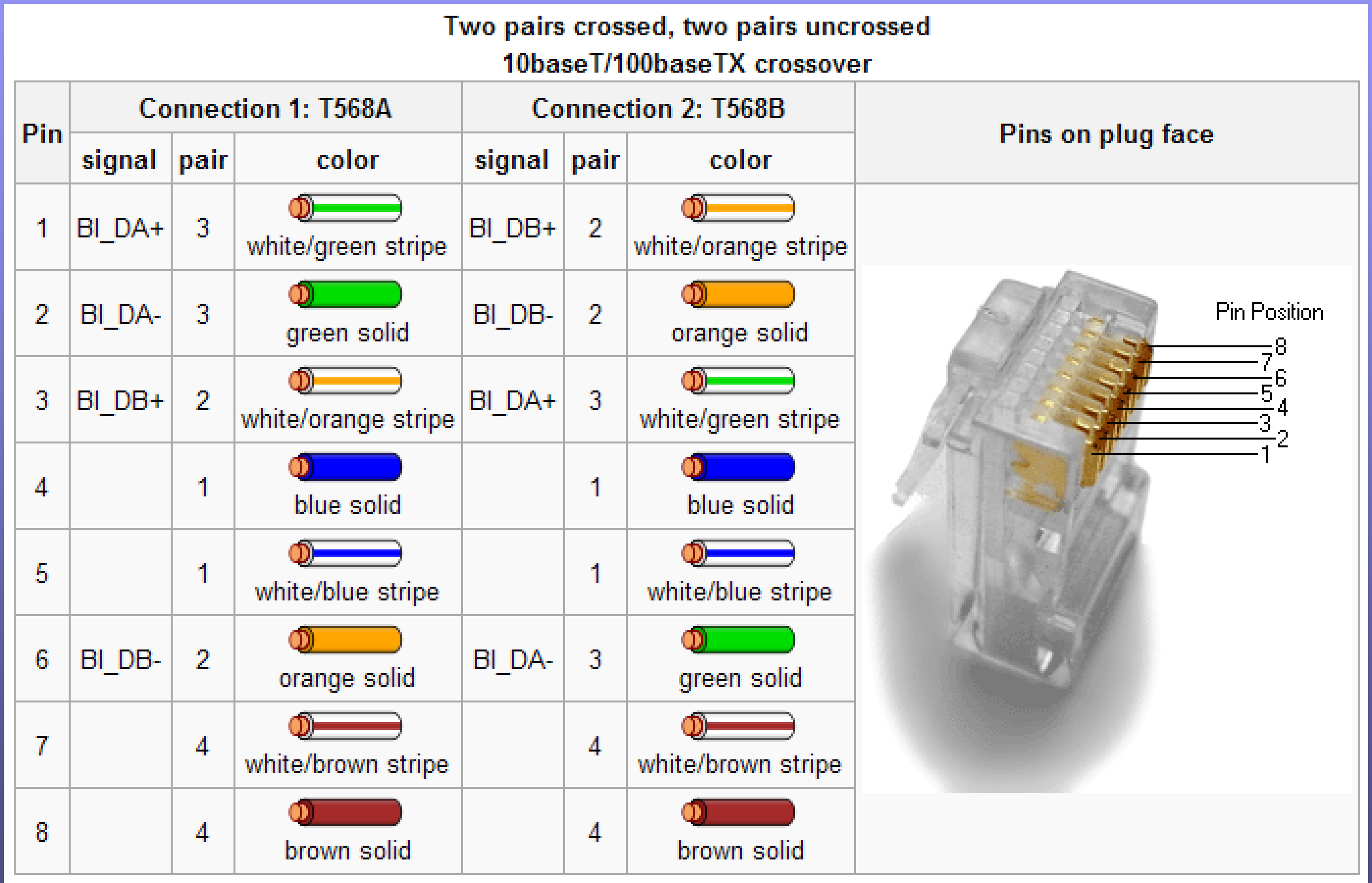
Pin	Pair	Wire	Color
1	3	1	white/green
2	3	2	green
3	2	1	white/orange
4	1	2	blue
5	1	1	white/blue
6	2	2	orange
7	4	1	white/brown
8	4	2	brown



TIA/EIA-568-B.1-2001 T568B Wiring

Pin	Pair	Wire	Color
1	2	1	white/orange
2	2	2	orange
3	3	1	white/green
4	1	2	blue
5	1	1	white/blue
6	3	2	green
7	4	1	white/brown
8	4	2	brown

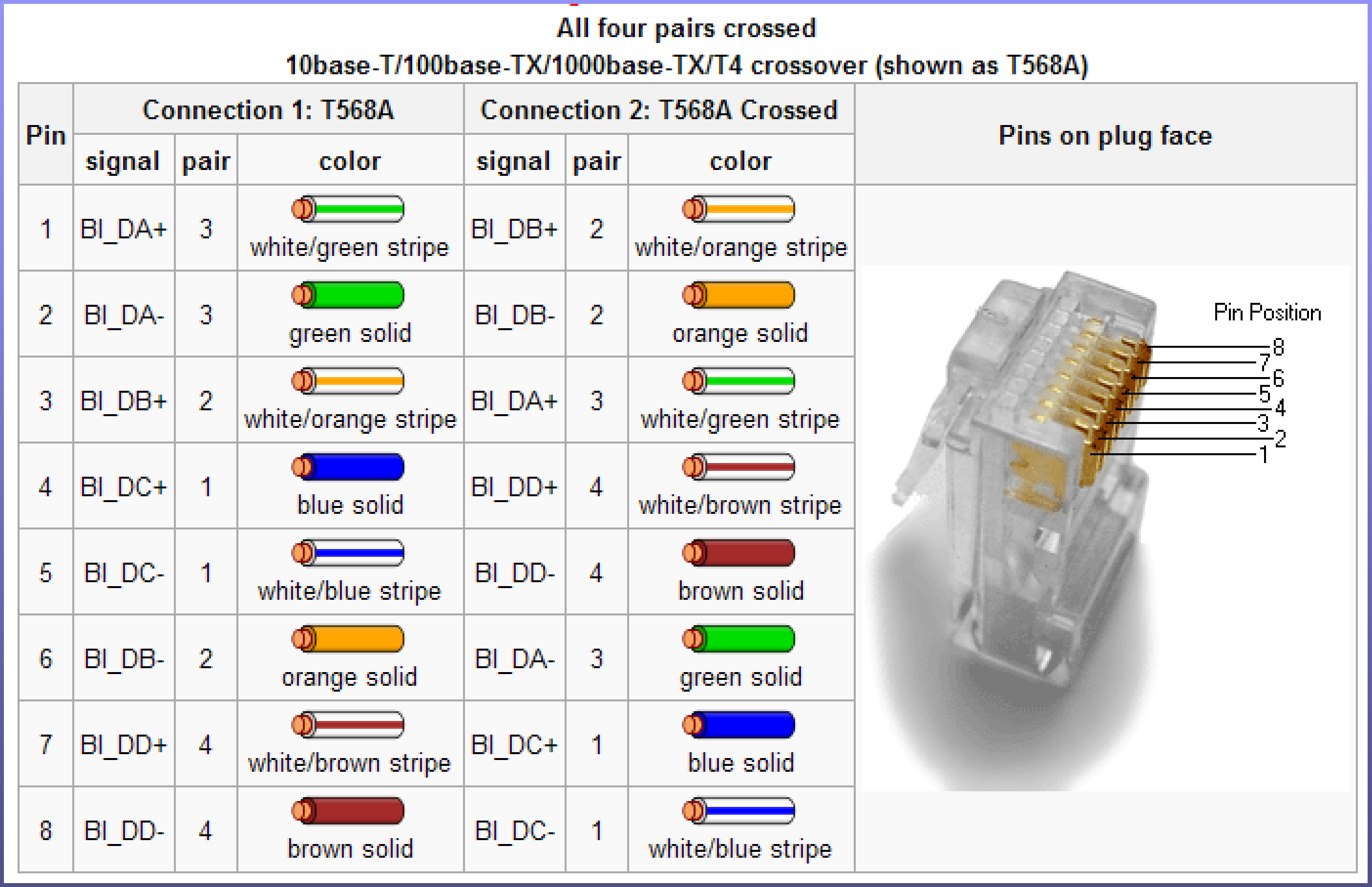
100Mb Crossover



Two pairs crossed, two pairs uncrossed
10baseT/100baseTX crossover

Pin	Connection 1: T568A			Connection 2: T568B			Pins on plug face
	signal	pair	color	signal	pair	color	
1	BI_DA+	3	white/green stripe	BI_DB+	2	white/orange stripe	
2	BI_DA-	3	green solid	BI_DB-	2	orange solid	
3	BI_DB+	2	white/orange stripe	BI_DA+	3	white/green stripe	
4		1	blue solid		1	blue solid	
5		1	white/blue stripe		1	white/blue stripe	
6	BI_DB-	2	orange solid	BI_DA-	3	green solid	
7		4	white/brown stripe		4	white/brown stripe	
8		4	brown solid		4	brown solid	

1Gb Crossover Type-A



All four pairs crossed

10base-T/100base-TX/1000base-TX/T4 crossover (shown as T568A)

Pin	Connection 1: T568A			Connection 2: T568A Crossed			Pins on plug face
	signal	pair	color	signal	pair	color	
1	BI_DA+	3	white/green stripe	BI_DB+	2	white/orange stripe	
2	BI_DA-	3	green solid	BI_DB-	2	orange solid	
3	BI_DB+	2	white/orange stripe	BI_DA+	3	white/green stripe	
4	BI_DC+	1	blue solid	BI_DD+	4	white/brown stripe	
5	BI_DC-	1	white/blue stripe	BI_DD-	4	brown solid	
6	BI_DB-	2	orange solid	BI_DA-	3	green solid	
7	BI_DD+	4	white/brown stripe	BI_DC+	1	blue solid	
8	BI_DD-	4	brown solid	BI_DC-	1	white/blue stripe	

Cisco 3 Layer Model

- This is more of a legacy design, but you may still run into it.
- Core – Switched only – high speed!
- Distribution – Routing – traffic decisions are made here.
- Access – User connections – Traffic marking.
- This is a Cisco specific model, though Mikrotik is attempting to move to this very design. Cisco has long had Fast switching and CEF, where as MTK has done everything in CPU with no optimizations. With the advent of MPLS integration in the MTK OS, they want you to enable this and basically do a form of switching across your core to speed performance.

IP Addressing - The Post Office

- The aggregate network your IP address resides in is like your zip code, it gets the mail to the right post office.
- The network portion of your IP address sorts the mail at the post office to the right truck.
- The host portion of your IP address gets the mail to your mail box.

IP Address Classes

- There are 5 classes, A – E
- A is 0.0.0.0 - 127.255.255.255
- B is 128.0.0.0 - 191.255.255.255
- C is 192.0.0.0 - 223.255.255.255
- D is 224.0.0.0 - 239.255.255.255 - Multicast
- E is 240.0.0.0 - 255.255.255.254 - Experimental

Special Addressing

- RFC1918 addressing is private, non internet routable address space.
  - 10.0.0.0/8
  - 172.16.0.0/12
  - 192.168.0.0/16
- 127.0.0.1 is the IPv4 loopback address .

IP Address Structure

- Example IP is 192.168.0.1 255.255.255.0
- Network portion is 192.168.0
- Host portion is .1
- Subnet mask is 255.255.255.0
- Network portion is determined by the subnet mask.

How to Subnet

- My favorite book example, and the way I learned was via Todd Lammle’s Sybex CCNA book.
- http://www.learntosubnet.com/
- http://lantech.geekvenue.net/chucktips/jason/chuck/1022445898/index_html
- http://www.speedguide.net/read_articles.php?id=1883

Subnetting in Your Head
Your Fingers are Your Friends

- How to determine subnet size
  - How many hosts do we need in our subnet?
    - Remember we lose 2 IP addresses per subnet; one for network and one for broadcast.
  - How many different subnets do we need?

Netmask Memorization Chart

Subnet Values	Number of IPs	# of bits to add to the default subnet mask
128	128	1
192	64	2
224	32	3
240	16	4
248	8	5
252	4	6
254	2	7

You have to memorize the subnet values…this is unavoidable. The trick is to count these on your fingers as you go. If you can remember that the subnet value and number of IPs both start at 128, then you are golden. As you count your fingers, divide the number of IPs in half. Once you get to the number you want, recount to the same finger by the subnet values.

Finger-sub Example 1

- Host network is 10.0.0.0/8 or 255.0.0.0
- I need a small subnet that only has 28 users.
- Lets find our subnet mask by counting on our fingers. Finger 1 is 128, finger 2 is 64, finger 3 is 32, finger 4 is 16. That means we stop at finger 3 because we need at least 28 IP addresses.
- So, starting from finger 1 we count our subnets: finger 1is128, finger 2 is 192, finger 3 is 224. Our subnet mask will be 255.255.255.224.

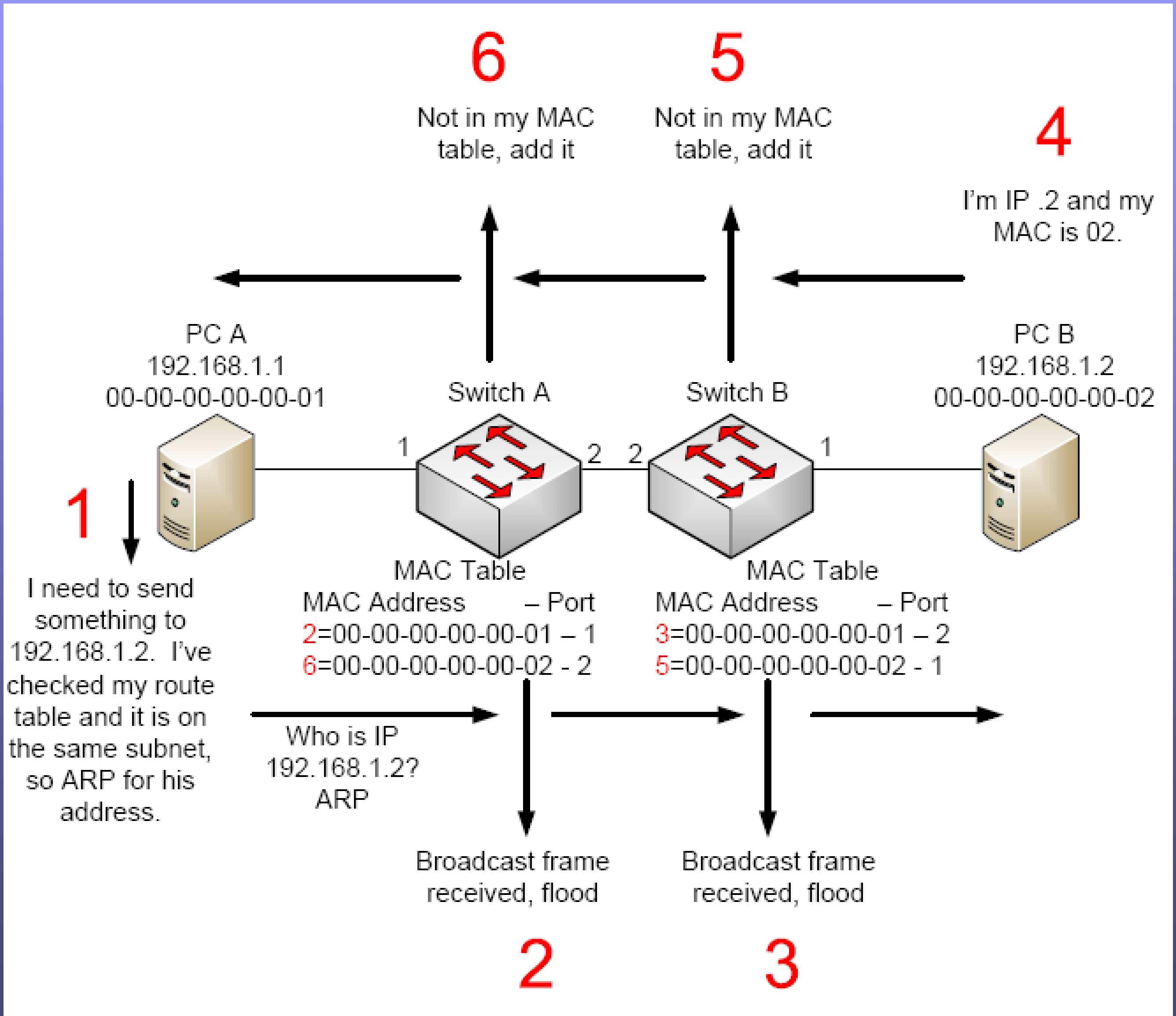
More Subnetting Terms

- VLSM – Variable Length Subnet Mask. This generally refers to subnetting a network address beyond it's classful boundary.
- CIDR – Classless Inter-Domain Routing. Uses the same concepts as VLSM to aggregate networks into non-classfull blocks.
- Subnet Zero – Cisco says subnet zero is "If a network address is subnetted, the first subnet obtained after subnetting the network address is called subnet zero." The command to allow this behavior is "ip subnet-zero". This command has been default for ages in IOS.

Switching

- The basic function of a switch is to provide ethernet connectivity for a LAN segment.
- Switches build a MAC address table (Cisco it’s called a CAM-Content Addressable Memory) dynamically.

MAC Learning Process



1

I need to send something to 192.168.1.2. I've checked my route table and it is on the same subnet, so ARP for his address.

Who is IP 192.168.1.2? ARP

2

Broadcast frame received, flood

3

Broadcast frame received, flood

4

I'm IP .2 and my MAC is 02.

5

Not in my MAC table, add it

6

Not in my MAC table, add it

MAC Table
MAC Address – Port
2=00-00-00-00-00-01 – 1
6=00-00-00-00-00-02 - 2

MAC Table
MAC Address – Port
3=00-00-00-00-00-01 – 2
5=00-00-00-00-00-02 - 1

STP – Spanning Tree Protocol

- Another important switching function is loop avoidance. This is generally done with STP.
- 802.1D was the original STP version. Ratified in 1998. 5 STP states: disabled, blocking, listening, learning, forwarding. In 2004, 802.1D-2004 was released that replace the legacy STP with RSTP.
- 802.1W RSTP – Rapid STP. This runs a single instance per link. RSTP standardized Cisco features such as port fast/backbone fast/uplink fast. 3 STP state: discarding, learning, forwarding. There are 3 link types:Point-2-point(connects to another switch – designated as p2p when a BPDU is received), Shared(connects to a hub) and Edge(connects to singe host – designated with portfast command in Cisco).
- Port Roles
  - Legacy STP <> Rapid ST
    - Root <> Root –Port that leads to root bridge.
    - Designated <> Designated – Port that leads downstream and is forwarding.
    - Blocking <> Alternate – Alternate root port that is in blocking state, waiting for root port to fail so it can quickly transition to root port.
    - Blocking <> Backup – Backup downstream port that is in blocking, waiting for designated port to fail so it can quickly transition to designated port.
- 802.1S MST – Multiple ST – What this does is allow you to run multiple instances of STP on a single link. You specify which VLANs are members of which MST instance. This way you can loadbalance your STP traffic.

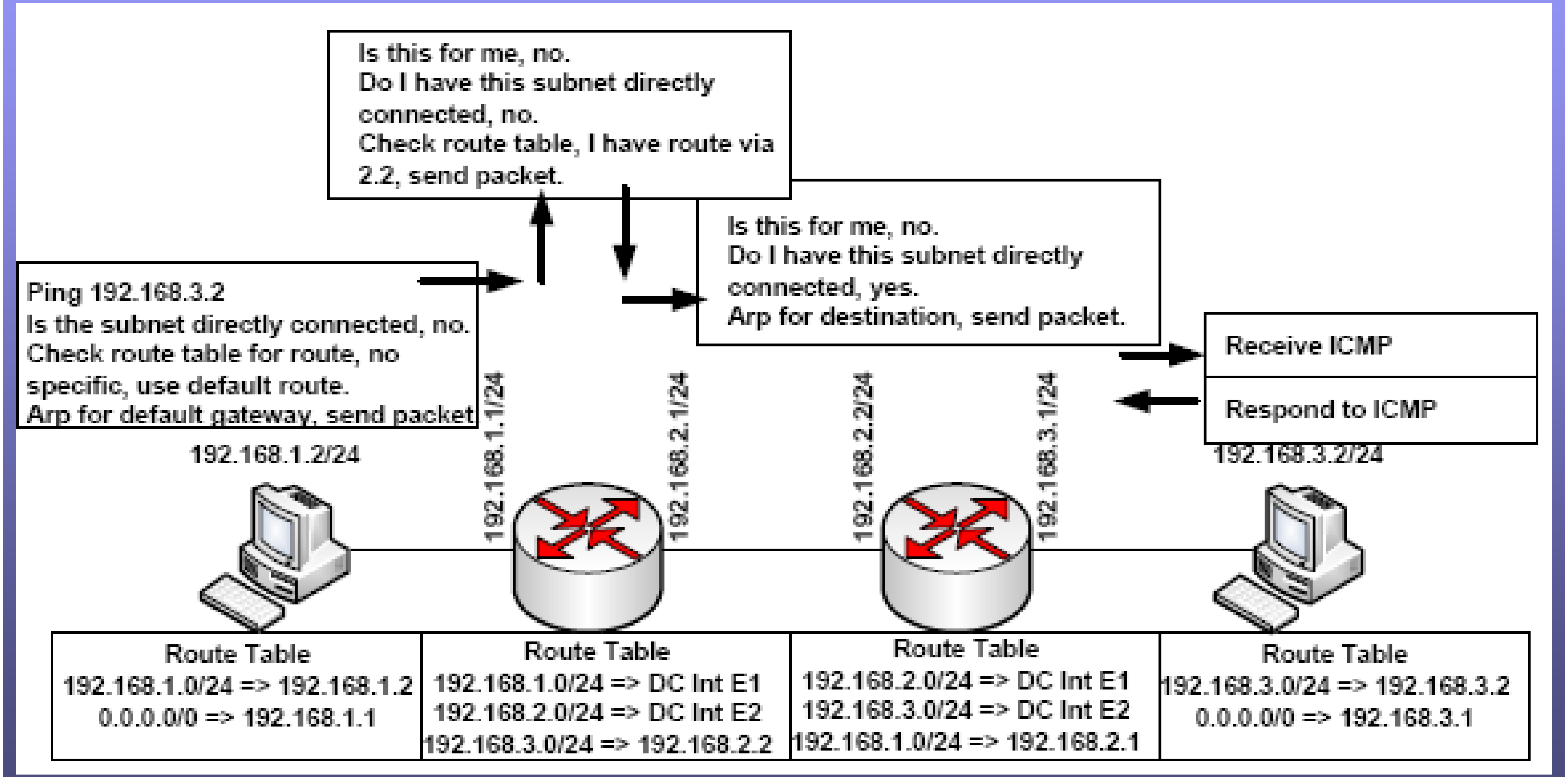
VLANs

- A VLAN is a method to tag traffic at L2.
- VLANs allow you to segment L2 traffic inside of a single switch or among a switched infrastructure.
- 802.1Q is the standards based VLAN trunking protocol.
- Trunking is a method to transfer tagged traffic from one switch to another while maintaining the VLAN tag on a packet.
- 802.1Q adds a field to the L2 ethernet frame, where as the Cisco proprietary ISL trunking protocol actually encapsulates the frame. Cisco => switchport mode trunk
- Tagged packets have the VLAN tag. Trunk Ports.
- Untagged packets have the VLAN tag stripped off. Access Ports. Cisco => switchport mode access

Routing

- A router’s basic job is to connect one LAN segment to another.
- Every port on a router breaks up collision domains and broadcast domains. No broadcast traffic is routed by default.
- Uses route table to determine how to move traffic.

Route Process



Ping 192.168.3.2
Is the subnet directly connected, no.
Check route table for route, no specific, use default route.
Arp for default gateway, send packet

Is this for me, no.
Do I have this subnet directly connected, no.
Check route table, I have route via 2.2, send packet.

Is this for me, no.
Do I have this subnet directly connected, yes.
Arp for destination, send packet.

Receive ICMP

Respond to ICMP

Route Table
192.168.1.0/24 => 192.168.1.2
0.0.0.0/0 => 192.168.1.1

Route Table
192.168.1.0/24 => DC Int E1
192.168.2.0/24 => DC Int E2
192.168.3.0/24 => 192.168.2.2

Route Table
192.168.2.0/24 => DC Int E1
192.168.3.0/24 => DC Int E2
192.168.1.0/24 => 192.168.2.1

Route Table
192.168.3.0/24 => 192.168.3.2
0.0.0.0/0 => 192.168.3.1

Building Route Table

- Static routes or dynamic routing protocols
  - – Static routes become cumbersome to maintain in large deployments.
  - – Dynamics(RIP, OSPF, BGP, EIGRP) scale for larger deployments. These are dynamic routing protocols. TCP/UDP are examples of routed protocols.
- Default route says, if you don’t match anything else, go this direction.

RIP – Routing Information Protocol

- RIP – Distance vector (hop count) – Bellman-ford algorithm. Inefficient broadcasts, send all routes every 30 seconds. 15 hop limitation. Classful.
- RIP V2 – Distance Vector. Uses multicast to distribute routes. 15 hop limitation. Classless.

OSPF – Open Shortest Path First

- Standards based.
- Link State protocol
- Concept of areas. Areas optimize route distribution and add stability
- Maintains an LSDB(Link State Database) of all connections within an area. All routers know all paths from all routers in same area. Allows each router to run the SPF calculation to find the best routes to install in their route table.
- Area 0 is the backbone area and all routers must traverse this area to reach any other area.
- Classless.
- Dijkstra algorithm.
- Uses protocol # 89 to transfer routing info.
- Uses DR and BDR on broadcast networks. Designated router receives updates from all other routers in area, then relays updates to all neighbors. Backup DR is poised to take the DRs place on failure.
- Maintains a neighbor or adjacency table. Routers that share the same subnet that are in at least a two-way state are considered neighbors.
- Uses Hellos for neighbor establishment and keep alives. High speed links default to 10 second hellos and dead timer at 40 seconds. Slow links default to 30 second hellos and 120 second dead timers.

OSPF Router Types

- Backbone router – Only in area 0.
- Area Border Router – Has interfaces in the backbone area and another area.
- ASBR – Has a connection that leads outside of the OSPF domain (Ex. connection to ISP).

OSPF LSA Types

- LSA stands for Link State Advertisement. This is how OSPF relays topology information between neighbors.
- Type 1 – Generated by all routers. Lists router’s neighbors and the cost to reach them.
- Type 2 – Generated only by DR. Lists all neighbors on a segment.
- Type 3 – Generated by ABR. Summary LSA. Strips topology info of the type 1/2 LSA. Sends prefix with cost into other areas.
- Type 4 – Generated by ASBR. ASBR summary. Created to give cost info to reach ASBR.
- Type 5 – Generated by ASBR. Used to advertise external routes.
- Type 7 – Generated by ASBR in a NSSA.

Area Types

- Standard
- Stubby – LSA type 5’s are removed and a default route is sent.
- Totally Stubby – LSA type 5 and 3 are removed and default is sent.
- Not So Stubby – LSA type 5s are blocked from entering area. If an ASBR is contained within the NSSA, instead of creating type 5 LSAs, it creates type 7 and are flooded throughout the area. When the type 7 hits an ABR, it is converted to a type 5 and sent to other areas to redistribute the external routes.
- Totally NSSA – Type 7s just like NSSA, only type 3s are blocked also.

Misc OSPF

- Network command does not tell OSPF what to advertise, rather it tells OSPF what interfaces to put in the OSPF process. You can alternately use the OSPF interface command in lieu of the network command.
- Passive interface is an interface that doesn’t participate in the process.
- Summarization can only be done at area boundaries.
- Virtual links can be used to transit a non-backbone area.

OSPF Troubleshooting

- Make sure that metrics match: timers, authentication, area, main subnet, whether a DR is elected or not, area type(stubby, NSSA). Technically MTU isn't part of the metrics that must match, but in Cisco, if they don't match your neighbors generally won't pass LSAs properly.

IGRP – EIGRP

- Cisco proprietary.
- Advanced Distance-vector or hybrid.
- Uses DUAL – Diffusing Update Algorithm.
- Neighbor table – contains neighbors.
- Topology table – contains routes from all neighbors.
- Metrics include – Bandwidth, Delay, Reliability, Load, MTU – Bandwidth/Delay are used by default. Cisco recommends not using the other metrics.

BGP

- Border Gateway Protocol
- This is the protocol the internet runs on.
- Built for stability.
- Path Vector.
- Uses Path Attributes to determine best route.
- The default PA is Autonomous system path(AS_PATH). Path refers to AS sequence.
- Forms neighbors via TCP port 179.
- Default hello interval is 60 seconds, default dead time is 180 seconds.
- Internal BGP neighbors iBGP is a neighbor in same AS.
- External BGP neighbors eBGP is a neighbor in a different AS.

BGP Neighbors

- TCP connection request must be sourced from and address in a neighbor statement.
- AS must match neighbor reference.
- Router IDs can’t be the same.
- Authentication must match (Cisco only supports MD5).
- BGP Open messages include the keepalive timer value. If they mismatch, they use the lowest value.

BGP NLRI

- The BGP topology table, also referred to as the BGP Routing Information Base holds Network Layer Reachability Information (NLRI).
- NLRI is an IP prefix and a prefix length.
- BGP does not technically advertise routes, rather it advertises Path Attributes along with NLRI that shares that same PA.

Route Table Decision Tree

- Next hop must be reachable.
- Use Shortest AS path.
- Prefer eBGP or iBGP.
- Lowest IGP metric to next hop.
- Choose BGP route with lowest Router ID.

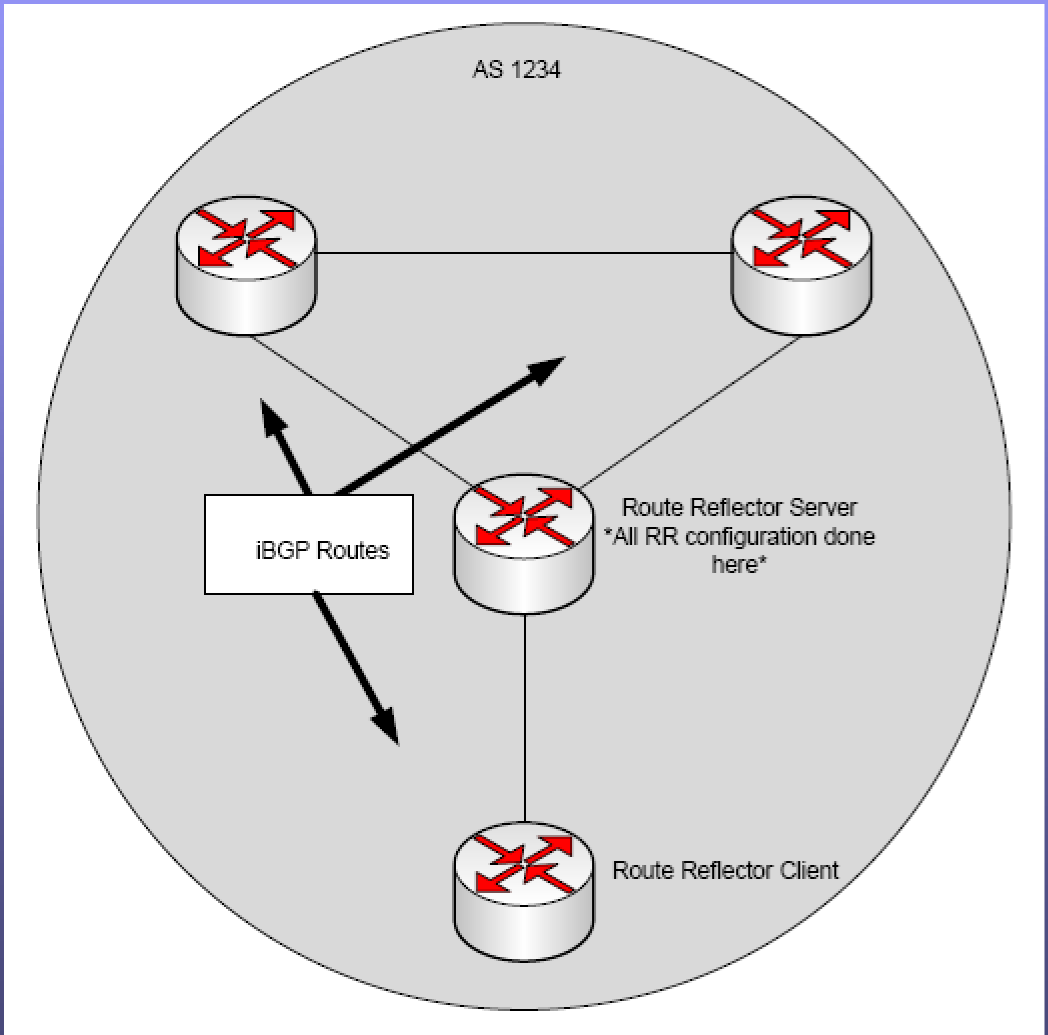
Route Advertising

- When sending to eBGP peer, next_hop is set to eBGP router.
  - Can be changed with
    - Cisco next-hop-unchanged
    - Mikrotik “nexthop choice” propogate
- When sending to iBGP peer, next_hop info is left intact.
  - Can be changed with
    - Cisco next-hop-self
    - Mikrotik “nexthop choice” force self

Route Reflection

- iBGP peers by default won't advertise routes learned via other iBGP peers. A full mesh is required in iBGP.
- Route Reflection is a way around that. If you have a stub peer, you can make it a route reflector client, and the route reflector server will advertise all iBGP routes to and from this peer to all of its peers.

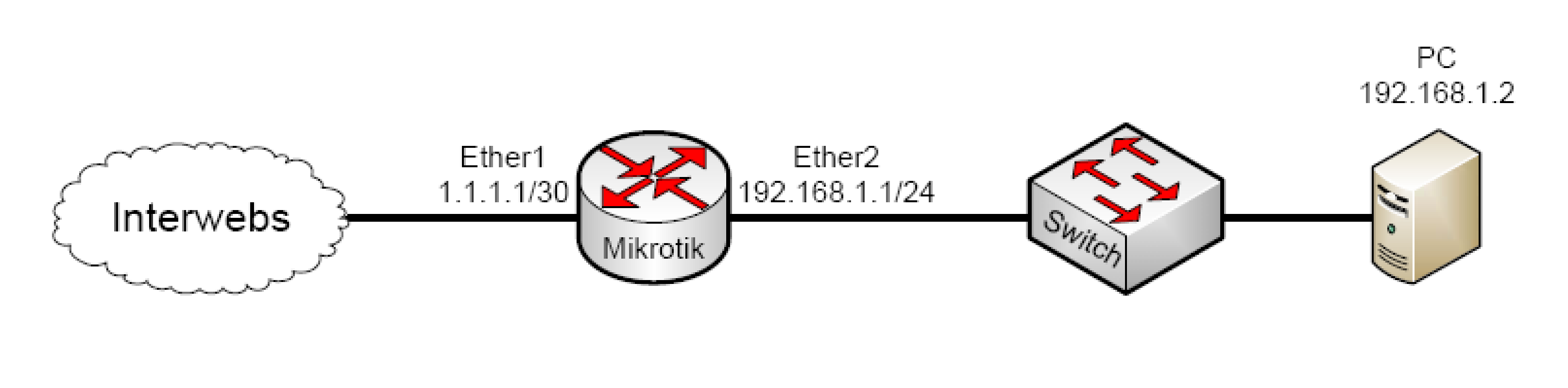
RR Continued



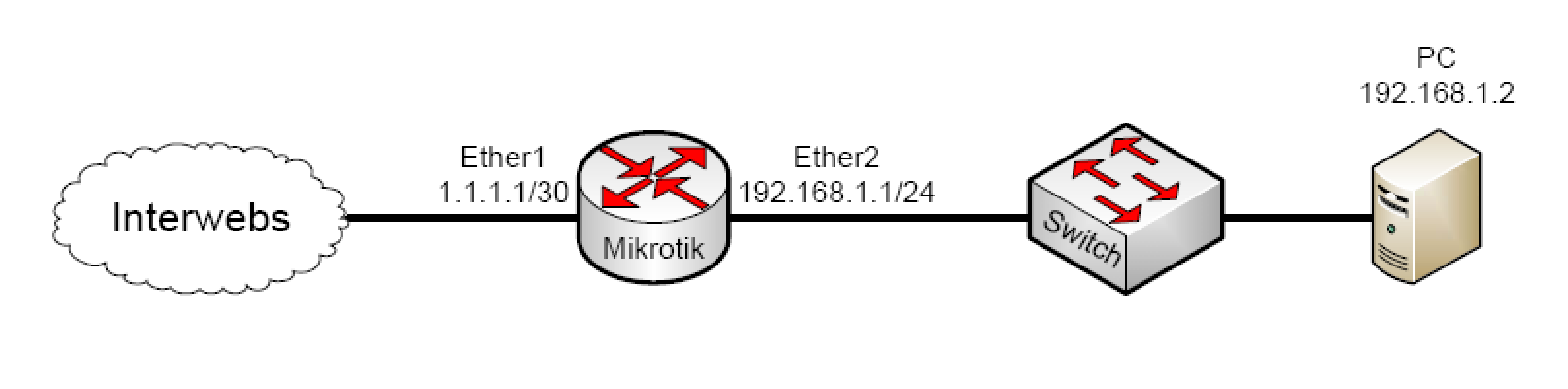
NAT

- Network Address Translation.
- This conserves public IP addressing.
- This allows two organizations that have overlapping address space to merge.
- Take an IP or pool of IPs and translate their address to a new IP or pool of IP addresses.
- Types:
  - Static – This is your 1 to 1 natting. Single IP to single IP or single port to single port.
  - Dynamic – This is a pool of IP address natted to another pool of IPs. This would be when two orgs combine and have overlapping IP or if you have enough publics to hand a single public to a pool of addresses.
  - Overload or Masquerade. This is really PAT or Port Address Translation. Port Address Translation is a method to translate multiple private addresses to a single public IP.

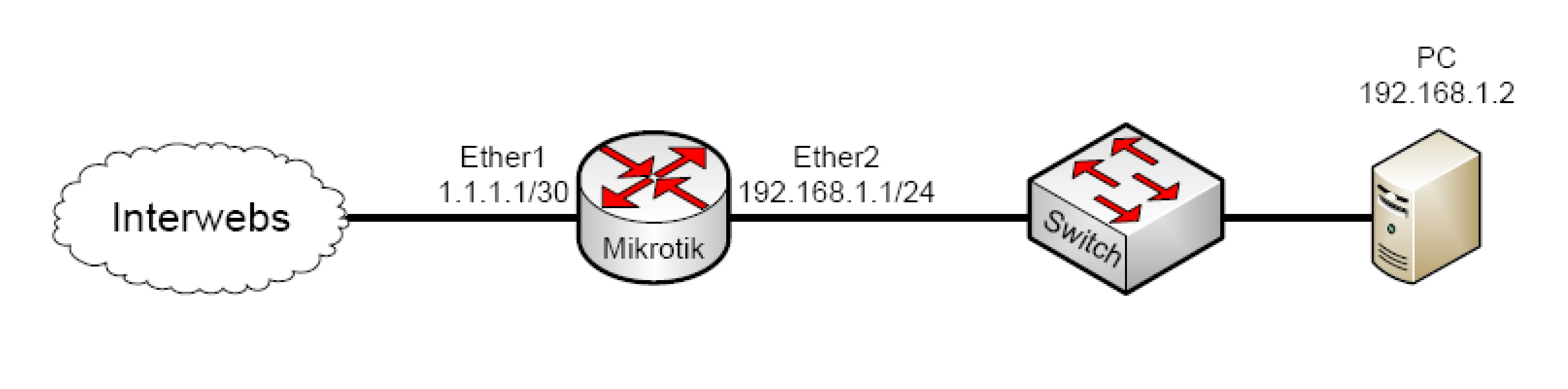
NAT


Interwebs
Ether1
1.1.1.1/30
Mikrotik
Ether2
192.168.1.1/24
Switch
PC
192.168.1.2

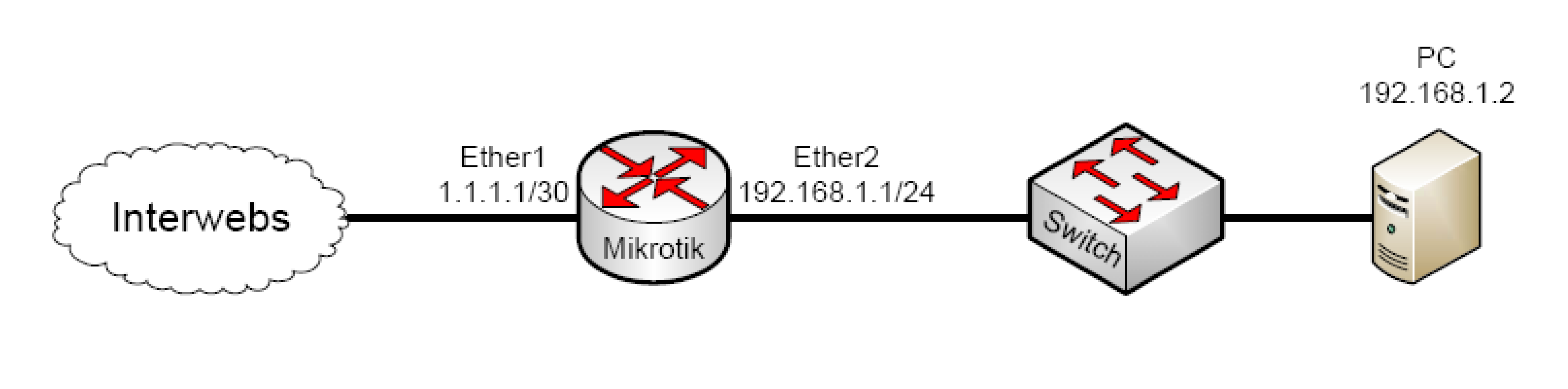
Basic Diagram



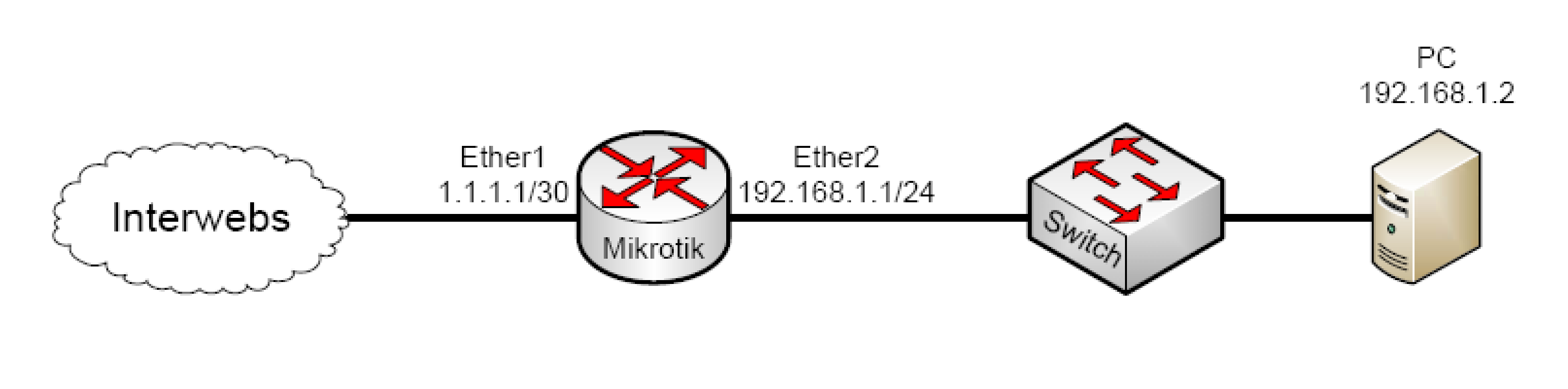
Basic Diagram 2



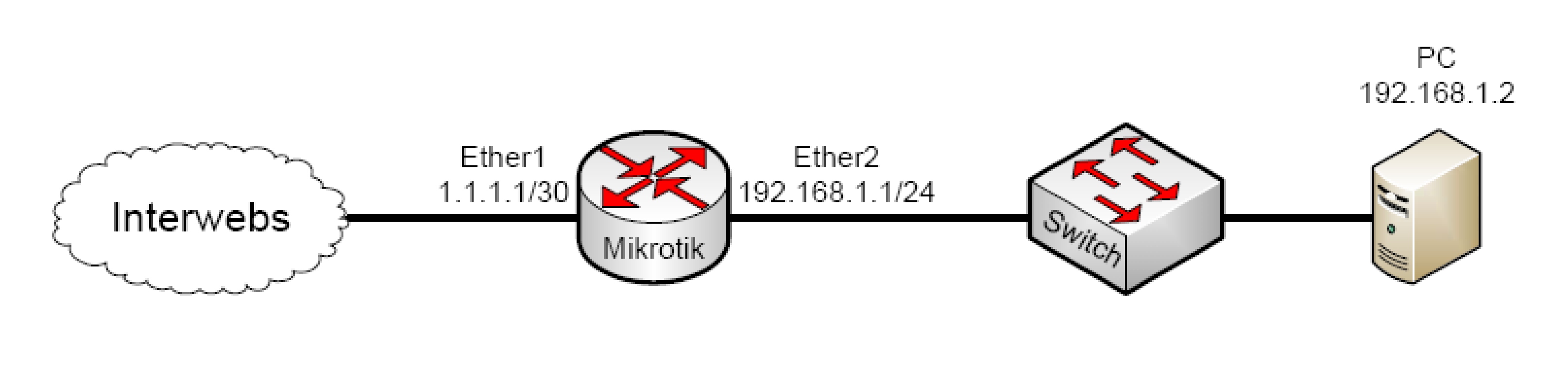
Basic Diagram 3



Basic Diagram 4



Basic Diagram 5


Interwebs
Ether1
1.1.1.1/30
Mikrotik
Ether2
192.168.1.1/24
Switch
PC
192.168.1.2