# default route

* the default route is a configuration of the Internet Protocol (IP) that establishes a forwarding rule for packets when no specific address of a next-hop host is available from the routing table or other routing mechanisms.
* The default route in Internet Protocol Version 4 (IPv4) is designated as the zero address, 0.0.0.0/0
* A route lookup that does not match any other rule falls back to this route

<https://www.juniper.net/documentation/us/en/software/junos/is-is/topics/concept/default-route-understanding.html>

# source NAT (Network Address Translation) on router

* Source NAT is most used for translating private IP address to a public routable address to communicate with the host.
* Translate a single IP address to another address (for example, to provide a single device in a private network with access to the Internet).
* Translate a contiguous block of addresses to another block of addresses of the same size.
* Translate a contiguous block of addresses to another block of addresses of smaller size.
* Translate a contiguous block of addresses to a single IP address or a smaller block of addresses using port translation.
* Translate a contiguous block of addresses to the address of the egress interface.

<https://www.juniper.net/documentation/us/en/software/junos/nat/topics/topic-map/nat-security-source-and-source-pool.html>

# Static routing

* Static routes are used in IP networks and allow very precise control over traffic going through a router.
* By default, static routes take precedence over routing protocols such as RIP or OSPF to communicate routing information between routers.
* Static routes are ideal for small networks with a limited number of paths and are particularly well suited for peripheral routers that are connected to one or more networks via only one router
* A disadvantage of static routes is its inability to adapt to router or link failures

<https://www.juniper.net/documentation/en_US/northstar4.3.0/topics/concept/ipmpls-static-route-overview.html>

# Connecting VMWW-nets to physical nets. VMWW bridge

???????????????????????????

# DHCP-service (Dynamic Host Configuration Protocol)

* The DHCP server, automatically assigns IP addresses and other network configurations like subnet mask, default gateway, DNS server, and more to the connected devices so they can exchange information.
* DHCP let the hosts get the necessary TCP/IP configuration data from the DHCP server.
* sing this protocol, the network administrators, don’t need to set a static IP for each device
* Components of DHCP
* **DHCP server.** The server device is in charge of answering an IP address request, provide an available IP address, store it for the time of the lease and renew it later. It will handle the communication with all the client devices. The server could be a computer or a part of the router.
* **DHCP client.** It must be present on the client devices (computer, mobile, IoT device, etc.). It will request an IP address and communicate with the DHCP server to get it with the rest of the data and confirm the process.
* **DHCP scope.** This is the range of IP addresses that the DHCP server can offer to the DHCP clients. Usually, the server will auto-assign addresses, starting from the smallest number, and going to the highest.
* **Subnet.** If the network is divided into pieces, there will be so-called subnets.
* Lease. That is the time period that indicates how long a client can use the assigned IP address before it expires.
* **DHCP relay.** The relay is in charge of communication between the DHCP server and the client. It will listen for messages and pass them to the right place.

<https://www.juniper.net/documentation/us/en/software/junos/dhcp/subscriber-mgmt-sessions/topics/ref/statement/dhcp-service-edit-system.html#dhcp-service__d10641e119>

<https://www.cloudns.net/blog/dhcp-server/>

# DHCP relay (Dynamic Host Configuration Protocol)

* A Juniper Networks device operating as a DHCP relay agent forwards incoming requests from BOOTP and DHCP clients to a specified BOOTP or DHCP server. Client requests can pass through virtual private network (VPN) tunnels.
* You cannot configure a single device interface to operate as both a DHCP client and a DHCP relay.
* On routers—In a typical carrier edge network configuration, the DHCP client is on the subscriber’s computer, and the DHCP relay agent is configured on the router between the DHCP client and one or more DHCP servers.
* The following steps describe, at a high level, how the DHCP client, DHCP relay agent, and DHCP server interact in a configuration that includes two DHCP servers.
* The DHCP client sends a discover packet to find a DHCP server in the network from which to obtain configuration parameters for the subscriber (or DHCP client), including an IP address.
* The DHCP relay agent receives the discover packet and forwards copies to each of the two DHCP servers. The DHCP relay agent then creates an entry in its internal client table to keep track of the client’s state.
* In response to receiving the discover packet, each DHCP server sends an offer packet to the client. The DHCP relay agent receives the offer packets and forwards them to the DHCP client.
* On receipt of the offer packets, the DHCP client selects the DHCP server from which to obtain configuration information. Typically, the client selects the server that offers the longest lease time on the IP address.
* The DHCP client sends a request packet that specifies the DHCP server from which to obtain configuration information.
* The DHCP relay agent receives the request packet and forwards copies to each of the two DHCP servers.
* The DHCP server requested by the client sends an acknowledgement (ACK) packet that contains the client’s configuration parameters.
* The DHCP relay agent receives the ACK packet and forwards it to the client.
* The DHCP client receives the ACK packet and stores the configuration information.
* If configured to do so, the DHCP relay agent installs a host route and Address Resolution Protocol (ARP) entry for this client.
* After establishing the initial lease on the IP address, the DHCP client and the DHCP server use unicast transmission to negotiate lease renewal or release. The DHCP relay agent “snoops” on all of the packets unicast between the client and the server that pass through the router (or switch) to determine when the lease for this client has expired or been released. This process is referred to as lease shadowing or passive snooping.

<https://www.juniper.net/documentation/us/en/software/junos/dhcp/topics/topic-map/dhcp-relay-agent-security-devices.html>

# Switching on SRX. Destination NAT (Network Address Translation)´

Destination NAT rules specify two layers of match conditions:

* Traffic direction—Allows you to specify from interface, from zone, or from routing-instance.
* Packet information—Can be source IP addresses, destination IP address or subnet, destination port numbers or port ranges, protocols, or applications.

The actions you can specify for a destination NAT rule are:

* off—Do not perform destination NAT.
* pool—Use the specified user-defined address pool to perform destination NAT.

The main configuration tasks for destination NAT are as follows:

* Configure a destination NAT address pool that aligns with your network and security requirements.
* Configure destination NAT rules that align with your network and security requirements.
* Configure NAT proxy ARP entries for IP addresses in the same subnet of the ingress interface.

<https://www.juniper.net/documentation/us/en/software/junos/nat/topics/topic-map/security-nat-destination.html>

# OSPF (Open Shortest Path First) routing protocol

* Open Shortest Path First (OSPF) is one of the Interior Gateway Protocol (IGP), which helps to find the best routing path between the source and the destination router using its own shortest path first (SPF) algorithm. It is a Link-state routing protocol that is used to distribute routing information about data packets within a large Autonomous System.
* **Backbone Area:** It is also known as area0 or area 0.0.0.0; it forms the very core of an OSPF network, and all other areas of the network are connected to the backbone area. It is responsible for distributing routing information between areas that are not backbone area types.
* **Stub Area:** In the case of Stud Area, routing in the area is entirely on the basis of a default route. It is an area that does not receive advertisements external to the autonomous system (AS)
* Not So Stubby Areas: NSSA is a type of stub that is able to import AS external routes and send them to any other area. However, it is unable to receive AS external routes from other areas of the network.
* **Transit Areas:** It is an area with 2 or more OSPF border routers, and it can be used to pass network traffic from one adjacent area to another one. It does not originate traffic, and neither it is the destination of any such traffic.

# OSPF (Open Shortest Path First) Route redistribution

<https://www.juniper.net/documentation/en_US/junos/topics/example/isis-redistributing-ospf-routes.html>