ACLs (Access Control Lists)

Control access to nodes in the network, function as a packet filter instructing the router to permit or discard specific traffic.
Traffic can be filtered based on src/dst IP, src/dst layer 4 port numbers, ...etc.
Configured globally in the router in global config mode, are ordered sequence of ACEs (Access Control Entries).
ACLs must be applied to the interface after being created either inbound or outbound.
A max of one ACL can be applied to a single interface per direction duplicates are replaced.
If a packet doesn't match any of the entries in the ACL it will be denied (implicit deny).

Standard ACLs: match traffic based only on src IP only and can either be numbered or named.
Numbered can be (1-99), (1300,1999).
Command: access-list <number> {deny | permit} <ip> <wildcard-mask>.
Command: access-list <number> permit {any|0.0.0.0 255.255.255.255} .
Command: access-list <number> remark <remark> .
Command: show access-lists. Command: show ip access-lists.
Command: show running-config | include/section access-list.
Command: ip access-list standard <acl-name> to enter standard named ACL config mode**.**
Command: ip access-list standard <number> to enter standard numbered ACL config mode**.**
Command: no <entry-number> to delete a certain ACE in standard numbered ACL config mode**.**
Command: [optional entry-number] {deny | permt } <ip> <wildcard-mask> in acl config mode.
Command:ip access-group <number | name> {in | out } on interface.
Command:ip access-list resequence <acl-id> <starting-seq-num> <increment> in global config mode to re-sequence ACL.
With a 32 mask you don't have to specify a wildcard mask or put the word "host" before the ip address with no mask.
Standard ACLs should be applied as close to the destination as possible.
The router may re-order /32 entries to improve the efficiency of processing ACL without changing its effect.
Ping -t to ping forever until stopped.
When configuring or editing numbered ACLs from global config mode you can only delete the entire ACL.

Extended ACLs can be numbered or named of ranges 100-199, 2000-2699, match traffic based on more parameters as : Layer 4 protocol.port, src address, dest address.
Command: access-list <number> {deny | permit} <protocol> <src-ip> <dest-ip>. For extended number ACLs.
Command: ip access-list extended <number|name> . For extended number ACLs config mode.
Command: <seq-num optional>{deny | permit} <protocol> <src-ip> <dest-ip>.
Command: deny tcp <src-ip> eq/gt/lt/neq/range <src-port-num> <dest-ip> eq/gt/lt/neq/range <dst-port-num>.
We use ip protocol option if we don't care about the protocol.
In extended ACLs to specify a/32 src or dest you have to use the host option or specify the wildcard mask.
After destination ip address and/or destination port numbers there are many options to use to match as ack for TCP ack flag, fin for TCP fin flag, syn for TCP syn flag, ttl to match packets with a specific TTL value, DSCP to match packets with a specific DSCP value.
Extended ACLs should be applied as close to the source as possible to limit how far the packets in the network travel before it can be denied.

DNS (Domain Name System) lets you specify names instead of ip addresses as destination.