ACL notes

ACL Applications
Without ACLS, all packets could be transmitted to all parts of the network
You may want to deny telnet access to the router from all VLANs except the management VLAN

Classification
VPN – set what is considering interesting traffic (needs to be encrypted

Redistribution between routing protocols
Allow certain routes to be redistributed

NAT
Which packets need to be translated and which do not need to be translated

2 Steps
Create an ACL in global config mode
R1(config)#access-list 1 (permit/deny) 10.1.1.0 0.0.0.255 (uses wildcard mask)

Apply to an interface and specify if this is an inbound or outbound rule
R1(config-if)#ip access-list 1 in
Or
Access-group command

<u>Inbound ACLs</u>

- Applied inbound on an interface
- ACL is processed before traffic is routed
- If discarded, the packet will not have to be processed for routing
- If permitted, the packet will be processed for routing

Outbound ACLs
Routing performed first
Packet is then directed to an outbound interface
Permitted – packet transmitted
Denied – packet dropped

Its more efficient to apply ACLs inbound on interfaces as if the packet is denied no routing of that packet has to take place. Whereas, packets sent through an outbound ACL are first processed/routed and then checked against the ACL list before being directed to an outbound interface

Process
R1(config)#access-list <1-99> <100-199> Standard or Extended

Packets are evaluated from the top down
If there is a match (permit/deny) all further instructions in the ACL are ignored
IF line does not match, then the next line will be checked
The end of an ACL has an implicit deny all, packet is dropped if no lines above were matched

There must be at least one permit line in an access list, if not than all traffic will be blocked on the interface that has that access list applied

Standard vs Extended
<1-99> <100-199> Standard or Extended

Standard ACL

only checks the source IP address
permits or denies entire protocol suite (cannot specify port numbers, tcp/udp, protocols, appliations)

Extended ACL
Checks on both the source and destination addresses
Permit or Deny based on specific protocols and application

Two methods to identify standard / extended ACLs

Numbered
<1-99> Standard   Standard Expanded Range <1300-1999>
<100-199> Extended   Extended Expanded Range <2000-2699>
Named
Use alphanumeric characters
Can be named descriptively