Linux server - Manage basic networking & Security

---

1. **Full form of " ping ".**
    - The full form of PING is the Packet InterNet Groper.
2. **What is the use of " ping " command ?**
    - The "ping" command is used to test the reachability of a host or network device in a computer network, as well as to measure the round-trip time for data to travel from the source (your computer) to the destination (the target host) and back. It is one of the most basic and widely used network diagnostic tools.

3. **What is the meaning of "prefix" is ?**
    - a "prefix" generally refers to the initial part or directory structure that comes before the actual filename or path to a file or directory. It is the portion of the path that specifies the location of a file or directory relative to the root directory ("/") or the current working directory.

4. **Which protocol is used in PING ?**
    - PING is used for network diagnostics and testing network connectivity, primarily relies on the ICMP (Internet Control Message Protocol) protocol.

5. **Port number of ICMP ?**
    - The ICMP packet does not have source and destination port numbers because it was designed to communicate network-layer information between hosts and routers, not between application layer processes.

6. **What is network ID and broadcast ID in IP range ?**
    - In IP networking, the terms "network ID" and "broadcast ID" are related to the concept of IP address classes and subnetting. These terms help define the range of IP addresses within a particular network or subnet.

7. **What is gateway ?**
    - "gateway" refers to a device or a software component that serves as a bridge or intermediary between different networks, allowing data to flow between them. Gateways play a crucial role in routing data between networks with different network protocols, addressing schemes, or communication technologies.

Linux server - Manage basic networking & Security

---

8. **What is SeLinux?**
    - SELinux (Security-Enhanced Linux) is a security framework and access control mechanism implemented in the Linux kernel and used by many Linux distributions to enforce mandatory access control (MAC) policies. SELinux enhances the security of a Linux system by adding an additional layer of access controls beyond the traditional discretionary access control (DAC) model, which relies on file permissions and user privileges.

9. **Wright down the list of SELINUX modes and their uses.**
    - Enforcing Mode:
        - Enforces security policies by actively denying actions that violate the rules.
        - Logs policy violations for auditing and security enforcement.
        - Ideal for production environments where strict security is essential.
    - Permissive Mode:
        - Does not actively enforce security policies but logs policy violations.
        - Allows administrators to monitor and debug SELinux policies without blocking actions.
        - Suitable for testing, debugging, and policy development.
    - Disabled Mode:
        - Turns off SELinux entirely.
        - No access controls are enforced, and no policy violation logs are generated.
        - Used when SELinux is not needed for security or compatibility reasons but should be approached with caution.

10. **In which mode, reboot is required after modification?**
    - SELinux (Security-Enhanced Linux) is designed to allow for dynamic policy changes without requiring a system reboot. Changes to SELinux modes, policies, and configurations can typically take effect immediately. Reboots are generally not required for most SELinux modifications, except in specific scenarios such as major system updates or kernel changes. However, it's essential to consult documentation and guidelines relevant to your specific environment to ensure proper application of SELinux changes.

Linux server - Manage basic networking & Security

11.What is SeLinux Booleans?

- SELinux Booleans are settings or parameters that allow system administrators to modify the behavior of SELinux policies on a Linux system without having to write custom policy rules or scripts. Booleans are binary flags that can be toggled to enable or disable specific access controls or policies within SELinux. They provide a way to fine-tune SELinux policy enforcement to meet the security requirements and operational needs of a system.

12.Which command is used to check the selinux contents.

- To check the SELinux context of a file or directory on a Linux system, you can use the ls command with the -Z option (capital "Z"). This option displays the SELinux security context of the specified file or directory.
- ls -Z <file_or_directory>

13. What is firewall ? why we use

- firewall is a network security device or software application that serves as a protective barrier between trusted internal networks and untrusted external networks, such as the internet. Firewalls are used to enhance network security by:
- Packet Filtering: Examining and controlling individual data packets based on predefined rules.
- Access Control: Specifying which network services, ports, protocols, and IP addresses are allowed or denied access.
- Stateful Inspection: Tracking the state of active connections to make context-aware decisions.
- Intrusion Detection and Prevention: Detecting and blocking suspicious or malicious activity.
- Proxy Services: Acting as intermediaries to hide internal network details.
- Network Address Translation (NAT): Enabling multiple internal devices to share a single public IP address.
- Content Filtering: Blocking access to specific websites or content categories.
- VPN Support: Facilitating secure communication for remote users via Virtual Private Networks.
- Logging and Auditing: Maintaining logs of network activity for monitoring and security analysis.

Linux server - Manage basic networking & Security

---

15. Which command is used for graphically manage firewall?

- Firewall-config

16. Which command is used for command line manage firewall?

- FirewallD (Dynamic Firewall Management):
- To view current FirewallD rules: firewall-cmd --list-all
- To add, modify, or remove FirewallD rules: Use firewall-cmd with options like --add-service, --add-port, or --add-rich-rule. Changes can be applied immediately and persistently.
- To reload FirewallD rules and apply changes: Use firewall-cmd --reload.

17. What is the use of " –get-default-zone " ?

- The --get-default-zone option is used with the firewall-cmd command in FirewallD, which is a dynamic firewall management tool commonly used in modern Linux distributions. This option is used to query and retrieve the name of the default zone currently set in FirewallD.

18. Which command is used to manage IP addressing in inux 7.0 ?

- In Linux 7.0 and later versions, IP addressing and network configuration can be managed primarily using the nmcli command-line tool, which is a part of the NetworkManager suite. NetworkManager is the default network management service in many modern Linux distributions, including CentOS and RHEL (Red Hat Enterprise Linux).

19. By default which name will assign to network card in RHEL ?

- In Red Hat Enterprise Linux (RHEL) and many other Linux distributions, network interfaces are typically named using the Predictable Network Interface Names (PNI) scheme, also known as "systemd Predictable Network Interface Names."

20. Which command is used to add/create a new network connection?

- nmcli connection add con-name "ConnectionName" ifname "InterfaceName" type "ConnectionType" [ConnectionOptions]

21. From which command is used to show the network connection?

- nmcli connection show