BTA 2023 ©

Network Ports

NUCLEAR NOTES©

Network Protocol Ports and associated knowledge as fast as humanly possible

Black Tower Academy

ajay Menendez

DRAFT 1.1


EXISTENCE IS CONFUSING AND I'M USUALLY NOT GOING TO EXPLAIN IT WELL
OK

Network Ports Explained

First, lets get some things straight, there are PHYSICAL ports that exist on a Network Interface, like in your laptop, or in a switch or router, and then there are virtual ones that exist at the **Transport Layer (Layer 4)** of the OSI model. The Transport Layer is responsible for end-to-end communication, ensuring that data is transmitted and received correctly between devices. It uses port numbers to identify specific applications or services on the destination device, allowing multiple services to communicate simultaneously.

Protocols like **TCP (Transmission Control Protocol)** and **UDP (User Datagram Protocol)** are key transport layer protocols that use port numbers to direct traffic to the appropriate application on a device.

Physical vs. Virtual Ports

- **Physical Ports**: These are hardware interfaces on devices like switches, routers, or computers. Physical ports connect cables (Ethernet, USB, etc.) to enable communication between different network devices.
- **Virtual Ports**: These are logical, software-defined points of communication used by computers and devices to exchange data over a network. Each virtual port is associated with a specific service or application, identified by a **port number**. Virtual ports exist within the operating system's networking stack, enabling data transmission without needing physical cables.

How Virtual Ports Work

In networking, communication between devices (clients and servers) happens over virtual ports. Each device has 65,536 virtual ports (0-65535), and a service or application listens on one of these ports to receive incoming data.

For example:

- **Web Servers**: A web server typically listens on port 80 (HTTP) or 443 (HTTPS).
- **Mail Servers**: An email server might use port 25 (SMTP) for sending mail.

Virtual ports ensure that the right service on a device processes incoming traffic. If a device is running multiple services (e.g., web server, mail server, etc.), each service listens on a different virtual port, ensuring they don't interfere with each other.

How Virtual Ports Work

The range of 0 to 65,535 ports comes from the limitations of the **binary number system** used in computing. Here's a step-by-step explanation:

Binary Number System and Bits

- Computers operate using the **binary number system**, where each bit (binary digit) can either be 0 or 1.
- Each bit in binary can represent two possible values (0 or 1). When multiple bits are combined, they can represent a larger range of values.

16-bit Binary Number

Ports are represented using a **16-bit number** in the binary system. This means there are 16 places in which each bit can be either 0 or 1.

- A 16-bit binary number can represent values from **0000000000000000 (0)** to **1111111111111111 (65,535)** in decimal.

Calculating the Range

- The number of possible values you can represent with 16 bits is calculated as **2^16**.
    - 216=65,5362^{16} = 65,536216=65,536
    - Since the binary system starts from 0, the range of possible port numbers is from **0 to 65,535**.

Thus, the 16 bits give us a total of 65,536 possible values (including 0), leading to port numbers ranging from **0 to 65,535**.

Why 16 Bits for Ports?

The choice of using 16 bits for port numbers is part of the design of **TCP** and **UDP** protocols, where each port is identified by a 16-bit number, allowing devices to support up to 65,536 unique ports.

This range provides enough room for thousands of services to use different ports for communication, with:

- **0-1023** being **well-known ports** (reserved for standard services like HTTP, SSH, etc.).
- **1024-49151** being **registered ports** (used for less common services).
- **49152-65535** being **dynamic or private ports**, often used by applications for temporary connections.

In summary, the range of port numbers is determined by the number of possible values that can be represented using 16 bits in the binary number system, which is 65,536 values, corresponding to ports 0 through 65,535.

Standard vs. Non-Standard Ports

- **Standard Ports**: Some port numbers are reserved for well-known services, defined by IANA (Internet Assigned Numbers Authority). For instance:
  - Port 80 for HTTP
  - Port 443 for HTTPS
  - Port 22 for SSH
- **Non-Standard Ports**: You can configure services to use non-standard ports for various reasons, including security (to obscure services from attackers scanning for common ports) or to avoid conflicts when multiple services are running. For example:
  - Instead of running an SSH server on port 22, you could configure it to use port 2222.
  - A web server could listen on port 8080 instead of 80.

While changing ports doesn't inherently add security (security through obscurity), it can help reduce the attack surface in some cases.

Configuring and Accessing Services on a Non-Standard Port

Web Browser Access

When accessing a service on a non-standard port via a web browser, you append the port number to the IP address or domain, separated by a colon.

- Example:
  - Standard Port: `http://example.com` (defaults to port 80)

- Non-Standard Port: `http://example.com:8080` (explicitly accessing port 8080)

This tells the browser to connect to the service running on port 8080 rather than the default HTTP port 80.

CLI (Command Line Interface) Access

Using a command-line tool, such as `curl` or `telnet`, you can also specify a port number when accessing services.

- **Using `curl`**:
  To connect to a web service running on a non-standard port:

```
curl http://example.com:8080
```

Using `telnet`:
To connect to an open TCP port (like SSH or HTTP) for testing:

```
telnet example.com 8080
```

- This initiates a connection to the service on port 8080.

How to Configure a Service to Listen on a Non-Standard Port

Services like web servers or SSH servers can be configured to use non-standard ports. Below are examples of how to change the port configuration:

Web Server (Apache or Nginx)

- **Apache**: You can configure a non-standard port by modifying the configuration file (e.g., `httpd.conf` or `apache2.conf`):

```
Listen 8080
```

- This line tells Apache to listen on port 8080.

- **Nginx**: In the `nginx.conf` file, you would modify the `server` block:

```
server {
    listen 8080;
    server_name example.com;
}
```

SSH Server (Linux)

To change the SSH port from the default 22, modify the `/etc/ssh/sshd_config` file:

```
Port 2222
```

After changing the port, restart the SSH service for the changes to take effect:

```
sudo systemctl restart sshd
```

Technical Interview Points for Cybersecurity Entry-Level Candidates

1. **Purpose of Virtual Ports**: Be able to explain how virtual ports enable multiple services to run on a single device, each with its own dedicated communication channel.
2. **Standard and Non-Standard Ports**: Understand the benefits and risks of using non-standard ports, especially from a security standpoint.
3. **Port Scanning**: Explain that attackers often use tools like `nmap` to scan for open ports on a network, searching for vulnerable services.
4. **Firewall Configuration**: Discuss how firewalls can block or allow traffic based on port numbers. For example, firewalls may block inbound traffic on non-standard ports unless explicitly configured to allow it.
5. **Accessing Services on Non-Standard Ports**: Be able to demonstrate how to access services running on non-standard ports using both a browser and command-line tools.
6. **Configuring Services on Non-Standard Ports**: Be ready to describe the steps to change the port number for common services like web or SSH servers and mention that it requires updating configuration files and restarting services.
7. **Security Implications**: Acknowledge that while using non-standard ports can help obscure services from casual attackers, more robust security measures like firewalls, intrusion detection systems (IDS), and encryption should always be employed.

By understanding these concepts, you'll be well-prepared for a technical interview and demonstrate a solid grasp of how virtual network ports work, their practical uses, and their security implications.

Memorizing standard Internet ports is essential for passing the **Sec+**, **CySA+**, and **Net+** certifications, succeeding in technical interviews, and applying this knowledge in business for several key reasons:

1. Foundation for Networking Concepts

Standard Internet ports are fundamental to understanding how devices communicate over a network. Many network protocols, like HTTP (port 80), HTTPS (port 443), and SSH (port 22), rely on specific port numbers to function properly. Memorizing these ports helps you:

- Understand and troubleshoot communication between devices.
- Quickly identify what services are running on a system based on the ports being used.

This foundational knowledge is critical in certification exams that test your understanding of basic networking concepts and security protocols.

2. Network Security and Threat Detection

Understanding port numbers is key to securing a network and detecting threats, which is especially important for **Sec+** and **CySA+**. Security professionals need to:

- Recognize **common ports** to identify normal network traffic.
- Identify traffic on **non-standard ports**, which may signal a potential security threat (e.g., malware using non-standard ports to evade detection).
- Implement **firewall rules** to allow or block traffic on specific ports, helping secure critical services while preventing unauthorized access.

Memorizing ports ensures you can quickly analyze network behavior and identify suspicious activity.

3. Certification Requirements

For certifications like **Sec+**, **CySA+**, and **Net+**, exam questions often require knowledge of common port numbers. These certifications cover topics such as:

- Identifying protocols and their associated ports.
- Recognizing security vulnerabilities based on open ports.
- Configuring security appliances like firewalls or intrusion detection systems (IDS) that depend on port numbers for rules.

To pass the exams, you need to quickly recall common ports to answer questions related to networking, security controls, and threat management.

4. Technical Interviews

Many technical interview questions for roles in IT, cybersecurity, and networking focus on your knowledge of common protocols and their ports. Interviewers expect you to:

- Recognize ports used by critical services like DNS (53), SMTP (25), or RDP (3389).
- Demonstrate how to secure a network by configuring firewalls, access control lists (ACLs), or intrusion detection systems using port numbers.
- Troubleshoot network connectivity issues, which often involve identifying whether the correct ports are open or blocked.

Having memorized standard ports helps you answer these questions efficiently and demonstrate a strong understanding of networking principles.

5. Real-World Business Applications

In a business environment, understanding standard ports is crucial for:

- **Troubleshooting network issues**: If users report problems with services like email or web browsing, knowing the port numbers lets you verify if the correct ports are open or being blocked by a firewall.
- **Configuring network services**: When setting up or securing services, such as a web server or VPN, you need to ensure they are running on the correct ports or modify them for security reasons (e.g., using non-standard ports).
- **Responding to security incidents**: Many attacks target specific ports (e.g., brute force attacks on SSH on port 22). Knowing which services run on which ports helps you quickly assess the situation and take action.
- **Implementing security controls**: Businesses need to enforce strict policies regarding which ports are open, closed, or monitored. Firewalls and IDS/IPS systems require configuration based on port numbers to properly secure the network.

6. Efficiency and Proficiency

Memorizing these ports allows for **faster response times** in both exams and real-world scenarios. When working in the field, you need to act quickly when identifying and responding to network issues, securing services, or conducting threat assessments.

For example, if a server is experiencing unusual traffic on port 3389 (RDP), you can immediately recognize this as a remote desktop protocol service and investigate whether it's a legitimate use or a potential security threat.

Key Ports to Memorize

Some commonly used ports that are frequently asked about in exams and interviews include:

- **HTTP (80)** and **HTTPS (443)**: Web traffic.
- **FTP (20, 21)**: File transfers.
- **SSH (22)**: Secure shell access.
- **DNS (53)**: Domain name resolution.
- **SMTP (25)**: Email sending.
- **RDP (3389)**: Remote desktop access.
- **SMB (445)**: Windows file sharing.
- **POP3 (110)** and **IMAP (143)**: Email retrieval.
- **SNMP (161)**: Network monitoring.

By memorizing these ports, you will be well-prepared for certifications, interviews, and the responsibilities of a networking or cybersecurity professional in a business setting.

Introductory Ports (Need to KNOW)

- **FTP (File Transfer Protocol)**: Transfers files between client and server; Transport Protocol: TCP; Port: 20, 21.
- **SFTP (Secure File Transfer Protocol)**: Securely transfers files using SSH; Transport Protocol: TCP; Port: 22.
- **SSH (Secure Shell)**: Encrypted network administration and file transfer; Transport Protocol: TCP; Port: 22.
- **Telnet**: Remote login, non-secure; Transport Protocol: TCP; Port: 23.
- **SMTP (Simple Mail Transfer Protocol)**: Sends emails; Transport Protocol: TCP; Port: 25.
- **DNS (Domain Name System)**: Resolves domain names to IP addresses; Transport Protocol: UDP; Port: 53.
- **TFTP (Trivial File Transfer Protocol)**: Simplified, unsecured file transfer; Transport Protocol: UDP; Port: 69.
- **HTTP (Hypertext Transfer Protocol)**: Web traffic communication; Transport Protocol: TCP; Port: 80.
- **HTTPS (Hypertext Transfer Protocol Secure)**: Secure web traffic via TLS/SSL; Transport Protocol: TCP; Port: 443.
- **POP3 (Post Office Protocol v3)**: Retrieves emails from server; Transport Protocol: TCP; Port: 110.
- **IMAP4 (Internet Message Access Protocol v4)**: Retrieves and manages emails; Transport Protocol: TCP; Port: 143.
- **RDP (Remote Desktop Protocol)**: Remote desktop access; Transport Protocol: TCP; Port: 3389.
- **NTP (Network Time Protocol)**: Synchronizes time across network devices; Transport Protocol: UDP; Port: 123.
- **SNMP (Simple Network Management Protocol)**: Monitors and manages network devices; Transport Protocol: UDP; Port: 161.
- **LDAP (Lightweight Directory Access Protocol)**: Directory services access; Transport Protocol: TCP/UDP; Port: 389.
- **LDAPS (Lightweight Directory Access Protocol Secure)**: Secure directory services access; Transport Protocol: TCP; Port: 636.
- **Kerberos**: Authentication protocol using tickets; Transport Protocol: TCP/UDP; Port: 88.

Deeper Ports (Good to KNOW)

- **IPsec (Internet Protocol Security)**: Encrypts and authenticates IP packets, operates in Transport or Tunnel mode; Protocol: N/A (network layer).
- **IKE (Internet Key Exchange)**: Establishes security associations for IPsec; Protocol: UDP; Port: 500.
- **ESP (Encapsulating Security Payload)**: Provides encryption for IPsec; Protocol: N/A (part of IPsec).
- **GRE (Generic Routing Encapsulation)**: Tunnels packets across networks; Protocol: N/A.

- **L2TP (Layer 2 Tunneling Protocol)**: VPN tunneling protocol; Transport Protocol: UDP; Port: 1701.
- **PPTP (Point-to-Point Tunneling Protocol)**: VPN protocol; Transport Protocol: TCP; Port: 1723.
- **IKEv2 (Internet Key Exchange v2)**: VPN protocol, builds on IKE for IPsec; Transport Protocol: UDP; Port: 500.
- **SSL/TLS (Secure Sockets Layer / Transport Layer Security)**: Secures communication; Port: TCP; 443 (HTTPS).
- **DHCP (Dynamic Host Configuration Protocol)**: Assigns IP addresses automatically; Transport Protocol: UDP; Port: 67, 68.
- **SIP (Session Initiation Protocol)**: Manages VoIP communications; Transport Protocol: TCP/UDP; Port: 5060 (non-encrypted), 5061 (encrypted).
- **MGCP (Media Gateway Control Protocol)**: Controls VoIP gateways; Transport Protocol: UDP; Port: 2427, 2727.
- **H.323**: VoIP protocol for call setup; Transport Protocol: TCP; Port: 1720.
- **ICMP (Internet Control Message Protocol)**: Provides error messages and operational information; Protocol: N/A (network layer).
- **ARP (Address Resolution Protocol)**: Resolves IP addresses to MAC addresses; Protocol: N/A.
- **RARP (Reverse Address Resolution Protocol)**: Resolves MAC addresses to IP addresses; Protocol: N/A.
- **BGP (Border Gateway Protocol)**: Path-vector routing protocol for Internet routing; Transport Protocol: TCP; Port: 179.
- **OSPF (Open Shortest Path First)**: Link-state routing protocol; Protocol: N/A.
- **EIGRP (Enhanced Interior Gateway Routing Protocol)**: Cisco proprietary routing protocol; Protocol: N/A.
- **RIP (Routing Information Protocol)**: Distance-vector routing protocol; Transport Protocol: UDP; Port: 520.
- **MPLS (Multiprotocol Label Switching)**: Speeds up and manages traffic flow across the network; Protocol: N/A.
- **QoS (Quality of Service)**: Manages and prioritizes network traffic.
- **NAT (Network Address Translation)**: Translates private IP addresses to public IP addresses.
- **VLAN (Virtual Local Area Network)**: Creates logically segmented networks.
- **STP (Spanning Tree Protocol)**: Prevents network loops; Protocol: N/A.
- **VXLAN (Virtual Extensible LAN)**: Extends VLAN across data centers.
- **SYN Flood**: Type of DoS attack by overwhelming connections; Protocol: TCP.
- **UDP Flood**: DoS attack using UDP traffic; Protocol: UDP.
- **DNS Poisoning**: Redirecting traffic by corrupting the DNS cache.

Thank you for putting your trust in Black Tower Academy

We believe in QUALITY education and aim to make it affordable on the internet to all who wish to learn.

ajay Menendez