IEEE 802 Standards

IEEE 802 wireless standards

By **Alexander S. Gillis,** Technical Writer and Editor

IEEE 802 is a collection of networking standards that cover the physical and data-link layer specifications for technologies such as Ethernet and wireless. These specifications apply to local area networks (LAN) and metropolitan area networks (MAN). IEEE 802 also aids in ensuring multi-vendor interoperability by promoting standards for vendors to follow.

Essentially, the IEEE 802 standards help make sure internet services and technologies follow a set of recommended practices so network devices can all work together smoothly.

IEEE 802 is divided into 22 parts that cover the physical and data-link aspects of networking. The family of standards is developed and maintained by the IEEE 802 LAN/MAN Standards Committee, also called the LMSC. IEEE stands for Institute of Electrical and Electronics Engineers.

The set of standards started in 1979 with a "local network for computer interconnection" standard, which was approved a year later. The LMSC has made more than 70 standards for IEEE 802.

Why IEEE 802 standards are important

LMSC was formed in 1980 in order to standardize network protocols and provide a path to make compatible devices across numerous industries.

Without these standards, equipment suppliers could manufacture network hardware that would only connect to certain computers. It would be much more difficult to connect to systems not using the same set of networking equipment. Standardizing protocols help ensure that multiple types of devices can connect to multiple network types. It also helps make sure network management isn't the challenge it could be if it wasn't in place.

Examples of IEEE 802 uses

The IEEE 802 specifications can be used by commercial organizations to ensure their products maintain any newly specified standards. So, for example, the 802.11 specification that applies to Wi-Fi could be used to make sure Wi-Fi devices work together under one standard. In the same way, IEE 802 can help maintain local area network standards.

These specifications can also define what connectivity infrastructure will be used for -- individual networks, or those at a larger organizational scale.

The IEEE 802 specifications apply to hardware and software products. So, to ensure manufacturers don't have any input on the standards, there is a voting protocol in place. This makes sure that one organization does not influence the standards too much.

Working groups

The working groups are the different areas of focus within the 802 specifications. They are numbered from 802.1 onward.

802	Overview	Basics of physical and logical networking concepts.
802.1	Bridging	LAN/MAN bridging and management. Covers management and the lower sub-layers of OSI Layer 2, including MAC-based bridging (Media Access Control), virtual LANs and port-based access control. This also contains the time-sensitive networking task group.
802.2	Logical Link	Disbanded
802.3	Ethernet	"Grandaddy" of the 802 specifications. Provides asynchronous networking using "carrier sense, multiple access with collision detect" (CSMA/CD) over coax, twisted-pair copper and optical fiber media. Current speeds range from 10 Mbps to 10 Gbps. Check on the commonly used list of 802.3 technologies.
802.4	Token Bus	Disbanded
802.5	Token Ring	Disbanded
802.6	Distributed queue dual bus (DQDB)	Superseded. Revision of 802.1D. Superseded by 802.1D-2004.

802.7	Broadband LAN Practices	Disbanded
802.8	Fiber Optic Practices	Disbanded
802.9	Integrated Services LAN	Disbanded
802.10	Interoperable LAN security	Disbanded
802.11	Wi-Fi	Wireless LAN Media Access Control and Physical Layer specification. 802.11a, b, g, etc. are amendments to the original 802.11 standard. Products that implement 802.11 standards must pass tests and are referred to as "Wi-Fi certified."
802.11a		■ Specifies a PHY that operates in the 5 Ghz U-NII band in the US -- initially 5.15-5.35 AND 5.725-5.85 -- since expanded to additional frequencies ■ Uses Orthogonal Frequency-Division Multiplexing ■ Enhanced data speed to 54 Mbps ■ Ratified after 802.11b
802.11b		■ Enhancement to 802.11 that added higher data rate modes to the DSSS (Direct Sequence Spread Spectrum) already defined in the original 802.11 standard ■ Boosted data speed to 11 Mbps ■ 22 MHz Bandwidth yields 3 non-overlaping channels in the frequency range of 2.400 GHz to 2.4835 GHz

802.11d
802.11e
802.11g
802.11h
802.11i

802.11j	
802.11k	
802.11m	
802.11n	
802.11x	
802.12	Demand Priority
802.13	Not used
802.14	Cable modems
802.15	Wireless Personal Area Networks

802.15.1	Bluetooth
802.15.3a	UWB
802.15.4	ZigBee
802.15.5	Mesh Network
802.16	Wireless Metropolitan Area Networks
802.17	Resilient Packet Ring
802.18	Radio Regulatory TAG

802.19	Coexistence
802.20	Mobile Broadband Wireless Access
802.21	Media Independent Handoff
802.22	Wireless Regional Area Network
802.23	Emergency Services Working Group
802.24	Vertical Applications Technical Advisory Group (TAG)

Common Application Ports

The physical ports on your computer allow communicate with peripheral devices such as your keyboard and mouse and to connect with internet devices via Ethernet cables.

Witin computer networking, ports serve a similar purpose. When a computer system seeks to connect to another computer, the port serves as a communication endpoint. It is also possible for different services running on the same computer to expose various ports and communicate with one another using these ports. In simple terms, if a software application or service needs to communicate with others, it will expose a port. Ports are identified with positive 16-bit unsigned integers, ranging from 0 to 65535. Other services use this port number to communicate with the service or app. Port numbers are divided into three ranges: *well-known* ports, *registered* ports, and *dynamic* or *private* ports.

Well-known ports (also known as *system ports*) are numbered from 0 through 1023. For example, to connect to the host **example.com** via SSH, I would use this command:

```
ssh username@example.com -v
```

In this example, -v stands for verbose, and you should see output similar to this:

```
debug1: Connecting to example.com [<IP Addr>] port 22
```

As shown, SSH is trying to connect to **example.com** using port number 22. You may use the *-p* option to specify another port number; otherwise, SSH will default to 22.

The Internet Assigned Numbers Authority (IANA) has assigned port numbers to commonly used services like SSH, FTP, HTTP, HTTPS, and others. Here are some of the most common ones:

Port Number	Usage
20	File Transfer Protocol (FTP) Data Transfer
21	File Transfer Protocol (FTP) Command Control
22	Secure Shell (SSH)
23	Telnet - Remote login service, unencrypted text messages
25	Simple Mail Transfer Protocol (SMTP) E-mail Routing
53	Domain Name System (DNS) service
80	Hypertext Transfer Protocol (HTTP) used in World Wide Web
110	Post Office Protocol (POP3) used by e-mail clients to retrieve e-mail from a server

110	Post Office Protocol (POP3) used by e-mail clients to retrieve e-mail from a server
119	Network News Transfer Protocol (NNTP)
123	Network Time Protocol (NTP)
143	Internet Message Access Protocol (IMAP) Management of Digital Mail
161	Simple Network Management Protocol (SNMP)
194	Internet Relay Chat (IRC)
443	HTTP Secure (HTTPS) HTTP over TLS/SSL

In my work, I most commonly come across ports 80, 443, 20, 21, 22, 23, 25, and 53. Knowing these ports can help you work more efficiently.
What ports do you use the most, and why?

Cybercrime Implements in Pakistan

~~Update: (July 28, 2021):~~ As per a recently published new article by a renowned publication, the federal cabinet has given a green signal to the National Cyber Security Policy 2021, under which a national cyber security response framework will be created. The government has already established the Cyber Governance Policy Committee for the proper implementation of the new policy.

The policy is set to introduce strict actions against a cyberattack targeting any particular state institution, terming it as an "act of aggression against national sovereignty". The main purpose of the newly approved National Cyber Security Policy is to counter the different types of incidents that involve misuse of the information and other related communication technologies that could put financial matters and the security of the country in danger.

There are different types of cybercrimes, classified in the following categories:

- Hacking
- Identity theft
- Cyberbullying
- Cyberstalking
- Spoofing
- Financial fraud
- Digital Piracy
- Computer viruses and worms
- Malicious Software
- Intellectual property rights
- Money Laundering
- Denial of Service attack
- Electronic Terrorism
- Vandalism

Hacking: It is a type of cybercrime in which unauthorized access is gained to data in a system or computer.

Identity theft: It is the deliberate use of someone else's identity. The term identity theft was first used in 1964.

Cyberbullying: Also known as online bullying, cyberbullying, or is a form of harassment or bullying done using electronic means.

Cyberstalking: It is the use of the internet to stalk or harass someone. It involves false accusations, slander, and defamation.

Spoofing: It is a trick in which hackers deceive computer systems to gain illegitimate advantage and steal data from personal networks or websites.

Financial fraud: It is when someone steals money or deprives others of their assets through online means.

Digital Piracy: Also known as online piracy, it involves the practice of illegally downloading and distributing digital copyrighted content.

Computer viruses and worms: They are types of malware computer programmes that replicate themselves to spread and infect computer systems.

Malware: A software designed by cybercriminals to intentionally cause damage to the server, computer, client, or network.

Intellectual property rights: Intellectual property theft is defined as online theft of content or material that is copyrighted.

Money Laundering: It involves the use of the internet to launder money through different online payment systems.

Denial of service attack (DOS attack): It is a cyberattack to disrupt the targeted server and its traffic. It makes a network resource or machine unavailable to the intended users.

Electronic terrorism: Also known as cyberterrorism, electronic terrorism involves the use of the internet for violent acts. It involves potentially threatening someone or achieving ideological or political gains.

Online Vandalism: It is the action that involves the deliberate damage and destruction of your online material. It may also involve the modification of the online content on your website without your permission.

CYBERCRIME LAWS IN PAKISTAN

As of now, there are three cybercrime laws in Pakistan. These laws deal with different categories of internet crimes in Pakistan. They are listed as under:

- Electronic Transaction Ordinance (ETO) 2002
- Electronic / Cyber Crime Bill 2007
- Prevention of Electronic Crimes Act (PECA) 2016
- Electronic Transaction Ordinance (ETO) 2002

ELECTRONIC TRANSACTION ORDINANCE (ETO) 2002

Introduced in 2002, the Electronic transactions Ordinance (ETO) came out to be the first IT-relevant legislation. It was created by national lawmakers. It was a first step that served as a solid foundation for legal sanctity and protection of the local e-Commerce industry.

A large part of this cybercrime law in Pakistan was inspired by foreign law related to cybercrime. It has 43 sections dealing with different types of internet crimes in Pakistan. This cybercrime law in Pakistan deals with the following 8 main areas related to the e-Commerce industry.

CYBERCRIMES PUNISHMENTS IN PAKISTAN

Details regarding punishments for cybercrimes in Pakistan have been listed as under:

Type of Cybercrime	Punishment
Data Damage	3 years imprisonment or PKR 3 lac fine
Electronic Fraud	7 years imprisonment or PKR 7 lac fine
Electronic Forgery	7 years imprisonment or PKR 7 lac fine
Malicious Code	5 years imprisonment or PKR 5 lac fine
Cyberstalking	3 years imprisonment or PKR 3 lac fine
Spamming	3 years imprisonment or PKR 3 lac fine
Spoofing	6 months imprisonment or PKR 50 thousand fine
Cyberterrorism	10 years imprisonment or PKR 10 million fine

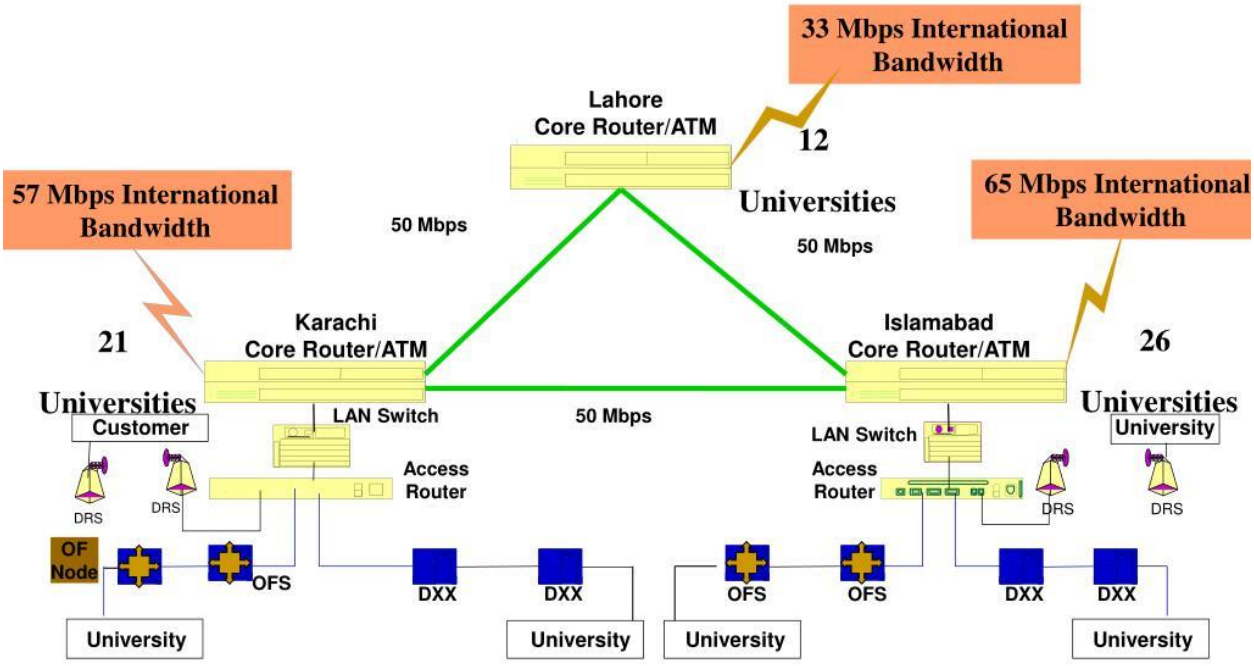
PERN Architecture

Pakistan Education & Research Network is the Research & Education Network of Pakistan which has been the integral part of the Government of Pakistan, IT Action Plan 2002. The National Research & Education Network (NRENs) by design are specialized educational intranet which are dedicated to support the needs of R&E communities within and outside the country. PERN, as any other global National Research & Education Network is a consortium of universities in Pakistan that is rendering different R&E and IT services as opted by the member universities over the PERN Network.

PERN Current Status

- 330 Universities\ Colleges connected in 66 Cities
  - o 228 Main Campuses
  - o 72 Sub Campuses
  - o 21 HED Punjab Government Colleges
  - o 9 HEC Khyber Pakhtunkhwa Colleges
- 50 Gbps International Bandwidth
- 31 New universities/ sub campuses will join PERN by August 2020
- 9 Gbps of Core Intranet Bandwidth Utilization
- International R&E link capacity of 2.5Gbps with TEIN (Trans Eurasia Information Network)

PERN Architecture



THE END!