

# COMPTIA NETWORK +

## [N10-008] WORKBOOK

[www.howtonetwork.com](http://www.howtonetwork.com)

# CONTENTS

## Module 1

<b>Lesson 1 OSI Model Layers and Encapsulation Concepts</b>	<b>31</b>
Agenda	32
<b>Topic 1: OSI Model Layers</b>	<b>33</b>
Overview	34
Physical Layer – Layer 1	35
Data Link Layer – Layer 2	36
Network Layer – Layer 3	37
Transport Layer – Layer 4	38
Session Layer – Layer 5	39
Presentation Layer – Layer 6	40
Application Layer – Layer 7	41
<b>Topic 2: Encapsulation &amp; Decapsulation</b>	<b>42</b>
Ethernet Header	43
IP Header	44
TCP Headers	46
UDP Headers	48
TCP Flags	49
Payloads	50
MTU	51
Summary	52
<b>Next Topic: Network Topologies and Network Types</b>	<b>53</b>
<b>Lesson 2 Network Topologies and Network Types</b>	<b>54</b>
Agenda	55
<b>Topic 1: Network Topologies</b>	<b>56</b>

Mesh	57
Star/Hub And Spoke	58
Bus	59
Ring	60
Hybrid	61
<b>Topic 2: Network Types &amp; Characteristics</b>	<b>62</b>
Peer-To-Peer	63
Client-Server	64
Peer-To-Peer	65
Wireless Local Area Network (WLAN)	66
Personal Area Network (PAN)	67
Campus Area Network (CAN)	68
Storage Area Network (SAN)	69
Software-Defined Wide Area Network	70
Multiprotocol Label Switching (MPLS)	71
Multipoint Generic Routing Encapsulation	72
<b>Topic 3: Service-Related Entry Point</b>	<b>73</b>
Demarcation Point And Smart Jack	74
Topic 4 Virtual Network Concepts	75
Vswitch	76
Virtual Network Interface Card (VNIC)	77
Network Function Virtualization (NFV)	78
Hypervisor	79
Topic 5 Provider Links	80
Service Provider Links	81
Summary	82
<b>Next Topic: Cables And Connectors</b>	<b>83</b>
<i>Lesson 3 Cables and Connectors</i>	<i>84</i>
Agenda	85

<b>Topic 1: Copper</b>	<b>86</b>
Copper - Twisted Pair	87
Copper – Other Types	88
Copper - Twisted Pair	89
<b>Topic 2: Fiber</b>	<b>90</b>
Single-Mode And Multimode	91
Single-Mode And Multimode	92
<b>Topic 3: Connector Types</b>	<b>93</b>
Local Connector (LC)	94
Straight Tip (ST)	95
Subscriber Connector (SC)	96
Mechanical Transfer (MT)	97
Registered Jack (RJ)	98
RJ11 / RJ45	99
F-Type Connector	100
Transceivers/Media Converters	101
Transceiver Type	102
<b>Topic 4: Cable Management</b>	<b>104</b>
Patch Panel/Patch Bay	105
Fiber Distribution Panel	106
Punchdown Blocks	107
<b>Topic 5 Ethernet Standards</b>	<b>108</b>
Ethernet Standards - Copper	109
Fiber Distribution Panel	110
Summary	111
<b>Next Topic: Ip Addressing Schemes</b>	<b>112</b>
 <i>Lesson 4 Ip Addressing Schemes</i>	 <b>113</b>
Agenda	114
<b>Topic 1: Public Vs. Private</b>	<b>115</b>

RFC 1918	116
Network Address Translation (NAT)	117
Port Address Translation (PAT)	118
<b>Topic 2: IPV4 vs. IPV6</b>	<b>119</b>
Automatic Private Ip Addressing (APIPA)	120
Extended Unique Identifier (EUI-64)	121
Multicast	122
Unicast	123
Anycast	125
Link Local	126
Loopback	127
Default Gateway	128
<b>Topic 3: IPV4 Subnetting</b>	<b>129</b>
Classless (Variable-Length Subnet Mask)	130
Classful	131
Classless Inter-Domain Routing (CIDR) Notation	132
<b>Topic 4: IPV6 Concepts</b>	<b>133</b>
Tunneling	134
Dual Stack	135
Shorthand Notation	136
Router Advertisement	137
Stateless Address Autoconfiguration (SLAAC)	138
<b>Topic 5: Virtual Ip (VIP)</b>	<b>139</b>
Virtual Ips (VIPS)	140
<b>Topic 6: Subinterfaces</b>	<b>141</b>
Subinterfaces	142
Summary	143
<b>Next Topic: Common Ports and Protocols</b>	<b>144</b>

<b>Lesson 5 Common Ports and Protocols</b>	<b>145</b>
Agenda	146
<b>Topic 1: Protocols</b>	<b>147</b>
File Transfer Protocol (FTP)	148
Secure Shell (SSH)	149
Secure File Transfer Protocol (SFTP)	150
Telnet	151
Simple Mail Transfer Protocol (SMTP)	152
Domain Name System (DNS)	153
Dynamic Host Configuration Protocol (DHCP)	154
Trivial File Transfer Protocol (TFTP)	155
Hypertext Transfer Protocol (HTTP)	156
Post Office Protocol V3 (POP3)	157
Network Time Protocol (NTP)	158
Internet Message Access Protocol (IMAP)	159
Simple Network Management Protocol (SNMP)	160
Lightweight Directory Access Protocol (LDAP)	161
Hypertext Transfer Protocol Secure (HTTPS)[SSL]	162
Https [Transport Layer Security (TLS)]	163
Server Message Block (SMB)	164
SYSLOG	165
SMTP TLS	166
Lightweight Directory Access Protocol (SSL) (LDAPS)	167
IMAP Over SSL	168
Pop3 Over SSL	169
Structured Query Language (SQL) Server	170
SQLNET	171
MYSQL	172
Remote Desktop Protocol (RDP)	173
Session Initiation Protocol (SIP)	174

Real-Time Transport Protocol (RTP)	175
Connectionless Vs. Connection-Oriented	176
Summary	177
<b>Next Topic: Network Services</b>	<b>178</b>
<b><i>Lesson 6 Network Services</i></b>	<b>179</b>
Agenda	180
<b>Topic 1: DHCP</b>	<b>181</b>
Scope, Exclusion Range, And Reservation	182
Dynamic and Static Assignment	183
Lease Time and Available Leases	184
Scope Options	185
DHCP Relay	186
IP Helper/UDP Forwarding	187
<b>Topic 2: DNS</b>	<b>188</b>
Record Types	189
Global Hierarchy – Root Servers	190
Internal vs. External	191
Zone Transfers	192
Authoritative Name Servers	193
Time To Live (TTL)	194
DNS Caching	195
Reverse DNS/Reverse Lookup/Forward Lookup	196
Recursive Lookup/Iterative Lookup	197
<b>Topic 3: DNS</b>	<b>198</b>
Stratum	199
Clients	200
Servers	201
Summary	202
<b>Next Topic: Corporate and Datacenter Network Architecture</b>	<b>203</b>

<b>Lesson 7 Corporate and Datacenter Network Architecture</b>	<b>204</b>
Agenda	205
<b>Topic 1: Three-Tiered</b>	<b>206</b>
Core	207
Distribution/Aggregation	208
Access/Edge	209
<b>Topic 2: Software-Defined Networking</b>	<b>210</b>
Software-Defined Network	211
Application Layer	212
Control Layer	213
Infrastructure Layer	214
Management Plane	215
<b>Topic 3: Spine And Leaf</b>	<b>216</b>
Top-of-Rack Switching	218
Backbone	219
<b>Topic 4: Spine And Leaf</b>	<b>220</b>
North-South	221
East-West	222
<b>Topic 5: Branch Office Vs. On-Premise Datacenter Vs. Colocation</b>	<b>223</b>
Branch Office Vs. On-Premises Datacenter Vs. Colocation	224
<b>Topic 6: Storage Area Networks</b>	<b>225</b>
Connection Types	226
Summary	227
<b>Next Topic: Cloud Concepts and Connectivity Options</b>	<b>228</b>
<b>Lesson 8 Cloud Concepts and Connectivity Option</b>	<b>229</b>
Agenda	230
<b>Topic 1: Deployment Models</b>	<b>231</b>
Public Cloud	232
Private Cloud	233

Community Cloud	234
Hybrid Cloud	235
<b>Topic 2: Service Models</b>	<b>236</b>
SAAS	237
IAAS	238
PAAS	239
DAAS	240
<b>Topic 3: Infrastructure As Code</b>	<b>241</b>
Infrastructure As Code (IAC)	242
<b>Topic 4: Connectivity Options</b>	<b>243</b>
Virtual Private Network (VPN)	244
Private-Direct Connections	245
<b>Topic 5: Multitenancy</b>	<b>246</b>
<b>Topic 6: Elasticity</b>	<b>248</b>
<b>Topic 7: Scalability</b>	<b>250</b>
<b>Topic 8: Security Implications</b>	<b>252</b>
Summary	255
<b>Next Topic: Networking and Networked Devices</b>	<b>256</b>

## Module 2

259

<b>Lesson 1 Networking and Networked Devices</b>	<b>259</b>
Agenda	260
<b>Topic 1: Networking Devices</b>	<b>261</b>
HUB	262
Layer 2 Switch	263
Layer 3 Capable Switch	264
Router	265
Access Point	266
Bridge	267
Wireless Lan Controller	268
Load Balancer	269
Proxy Server	271
Cable Modem	273
DSL Modem	274
Repeater	275
Voice Gateway	276
Media Converter	277
IDS/IPS	278
Firewall	279
VPN Headend	281
<b>Topic 2: Networked Devices</b>	<b>282</b>
Voice Over Internet Protocol (VOIP) Phone	283
Printer	284
Physical Access Control Devices	286
Cameras	287
HVAC Sensors	288
Internet Of Things (IOT) Devices	290
ICS/SCADA	291

Summary	292
<b>Next Topic: Routing and Bandwidth Management</b>	<b>293</b>
<b><i>Lesson 2 Routing and Bandwidth Management</i></b>	<b>294</b>
Agenda	295
<b>Topic 1: Routing</b>	<b>296</b>
Routing and Its Types	297
Static Routing	298
Dynamic Routing	299
Static Routing	300
Dynamic Routing Protocols	301
Link State	302
Distance Vector	305
Hybrid	308
Default Route	311
Administrative Distance	312
Exterior Vs. Interior	313
Time To Live	314
<b>Topic 2: Bandwidth Management</b>	<b>316</b>
Bandwidth Management	317
Traffic Shaping	318
Quality Of Service (QOS)	319
Summary	321
<b>Next Topic: Ethernet Switching Features</b>	<b>322</b>
<b><i>Lesson 3 Ethernet Switching Features</i></b>	<b>323</b>
Agenda	324
Data Virtual Local Area Network (VLAN)	325
Voice VLAN	327
Media Access Control (MAC) Address Tables	339

Power Over Ethernet (POE)/Poe Plus (POE+)	340
Spanning Tree Protocol (STP)	341
CSMA/CD	342
Address Resolution Protocol (ARP)	343
Neighbor Discovery Protocol	345
Summary	347
<b>Next Topic: Wireless Standards and Technologies</b>	<b>348</b>

<b><i>Lesson 4 Wireless Standards and Technologies</i></b>	<b>349</b>
Agenda	350
<b>Topic 1: Wireless Standards</b>	<b>351</b>
Wireless Standards	352
802.11A	353
802.11B	354
802.11G	355
802.11N	356
802.11AC	357
802.11AX	358
<b>Topic 2: Frequencies and Range</b>	<b>359</b>
2.4 Vs. 5.0 Ghz	360
<b>Topic 3: Channels</b>	<b>361</b>
Regulatory Impacts	362
<b>Topic 4: Channel Bonding</b>	<b>363</b>
Channel Bonding	364
<b>Topic 5: Service Set Identifier (SSID)</b>	<b>365</b>
Basic Service Set	366
Extended Service Set	367
Independent Basic Service Set (AD-HOC)	368
Roaming	369
<b>Topic 6: Antenna Types</b>	<b>371</b>

Omni	372
Directional	373
<b>Topic 7: Encryption Standards</b>	<b>374</b>
WPA2 Personal	375
WPA2 Enterprise	376
<b>Topic 8: Cellular Technologies</b>	<b>377</b>
CDMA	378
GSM	379
LTE	380
3G, 4G, 5G	381
<b>Topic 9: Mimo And Mu-Mimo</b>	<b>382</b>
MIMO	383
MU-Mimo	384
Summary	385
<b>Next Topic: Using Sensors And Statistics</b>	<b>386</b>

## Module 3

387

<b>Lesson 1 Using Sensors and Statistics</b>	<b>389</b>
Agenda	390
<b>Topic 1: Performance Metrics/Sensors</b>	<b>391</b>
Performance Metrics/Sensors – Device/Chassis	392
Performance Metrics/Sensors – Device/Chassis	393
Performance Metrics/Sensors – Network Metric	394
<b>Topic 2: SNMP</b>	<b>396</b>
SNMP	397
<b>Topic 3: Network Device Logs</b>	<b>400</b>
Network Device Logs	401
Syslog Severity Levels	402
<b>Topic 4: Interface Statistics/Status</b>	<b>403</b>
Interface Statistics/Status – Link Status	404
Interface Statistics/Status – Speed/Duplex	405
Interface Statistics/Status – Sent/Receive Traffic	406
Interface Statistics/Status - CRCS	407
Interface Statistics/Status – Counts	409
<b>Topic 5: Interface Errors Or Alerts</b>	<b>410</b>
Interface Errors Or Alerts – CRC Errors	411
Interface Errors Or Alerts – CRC Errors	412
Interface Errors Or Alerts – RUNTS	413
Interface Errors Or Alerts – Encapsulation Error	414
<b>Topic 6: Environmental Factors &amp; Sensors</b>	<b>415</b>
Environmental Factors and Sensors	416
<b>Topic 7: Baselines</b>	<b>418</b>
Netflow Data	420
<b>Topic 8: Netflow</b>	<b>420</b>
<b>Topic 9: Uptime/Downtime</b>	<b>422</b>

Summary	425
<b>Next Topic: Organizational Documents and Policies</b>	<b>426</b>
<b><i>Lesson 2 Organizational Documents and Policies</i></b>	<b>427</b>
Agenda	428
<b>Topic 1: Environmental Factors &amp; Sensors</b>	<b>429</b>
Change Management	430
Incident Response Plan	432
Disaster Recovery Plan	434
Business Continuity Plan	436
System Life Cycle	438
Standard Operating Procedures	440
<b>Topic 2: Hardening And Security Policies</b>	<b>442</b>
Password Policy	443
Acceptable Use Policy	445
Bring Your Own Device (BYOD) Policy	447
Remote Access Policy	449
Onboarding And Offboarding Policy	451
Security Policy	453
Data Loss Prevention Policy	455
<b>Topic 3: Common Documentation</b>	<b>457</b>
Physical Network Diagram	458
Logical Network Diagram	460
Wiring Diagram	461
Site Survey Report	462
Audit And Assessment Report	463
Baseline Configurations	464
<b>Topic 4: Common Agreements</b>	<b>465</b>
Non-Disclosure Agreement (NDA)	466
Service-Level Agreement (SLA)	467

Memorandum Of Understanding (MOU)	468
Summary	469
<b>Next Topic: High Availability and Disaster Recovery</b>	<b>470</b>
 <i><b>Lesson 3 High Availability and Disaster Recovery</b></i>	<b>471</b>
Agenda	472
<b>Topic 1: Load Balancing</b>	<b>473</b>
<b>Topic 2: Multipathing</b>	<b>475</b>
<b>Topic 3: Network Interface Card (NIC) Teaming</b>	<b>477</b>
<b>Topic 4: Redundant Hardware/Clusters</b>	<b>479</b>
<b>Topic 5: Facilities and Infrastructure Support</b>	<b>481</b>
Facilities & Infrastructure Support - UPS	482
Facilities & Infrastructure Support - PDUS	483
Facilities & Infrastructure Support-Generator	484
Facilities And Infrastructure Support - HVAC	485
Facilities And Infrastructure Support – Fire Suppression	486
<b>Topic 6: Redundancy And High Availability (HA) Concept</b>	<b>487</b>
Recovery Sites - Cloud	488
Recovery Sites - Hot	489
Recovery Sites - Warm	490
Recovery Sites – Cold	491
High Availability Configurations – Active/Active	492
High Availability Configurations-Active/Passive	493
High Availability Configurations – Multiple Isps	494
High Availability Configurations – Diverse Path	495
Recovery Protocols - FHRP	496
Recovery Protocols	497
High Availability Measurements - MTBF	498
High Availability Measurements - MTTR	499
Recovery Objectives - RPO	500

Recovery Objectives - RTO	501
<b>Topic 7: Network Device Backup/Restore</b>	<b>502</b>
Network Device Backup/Restore – State	503
Summary	505
<b>Next Topic: Common Security Concepts</b>	<b>506</b>

## Module 4

	507
<b>Lesson 1 Explain Common Security Concepts</b>	<b>509</b>
Agenda	510
<b>Topic 1: CIA Triad</b>	<b>511</b>
Confidentiality	513
Integrity	515
<b>Topic 2: Availability</b>	<b>517</b>
Threats	518
Internal Threats	519
External Threats	520
<b>Topic 3: Vulnerabilities</b>	<b>521</b>
Common Vulnerabilities And Exposures (CVE)	522
<b>Topic 4: Zero-Day</b>	<b>523</b>
Exploits	524
<b>Topic 5: Least Privileges</b>	<b>526</b>
Least Privileges	527
<b>Topic 6: Role-Based Access</b>	<b>528</b>
<b>Topic 7: Zero Trust</b>	<b>530</b>
<b>Topic 8: Defense In Depth</b>	<b>532</b>
Defense-In-Depth – Network Segmentation	533
Defense-In-Depth – Screen Subnet	534
Defense-In-Depth – Separation Of Duties	535
Defense-In-Depth – Network Access Control	536
Defense-In-Depth – Honeypot	537
<b>Topic 9: Authentication Methods</b>	<b>538</b>
Authentication Methods - Multifactor	539
Authentication Methods – Tacacs+	540
Authentication Methods – Single Sign-On	541
Authentication Methods - Radius	542

Authentication Methods – Single Sign-On	543
Authentication Methods - Radius	544
Authentication Methods - LDAP	545
Authentication Methods - Radius	546
Authentication Methods–Local Authentication	547
Authentication Methods – 802.1X	548
Authentication Methods - EAP	549
<b>Topic 10: Risk Management</b>	<b>550</b>
Security Risk Assessment-Threat Assessment	552
Security Risk Assessment–Vulnerability Assess	553
Security Risk Assessment–Penetration Testing	554
Security Risk Assessment – Posture Assess	555
Business Risk Assessment – Process Assessment	556
Business Risk Assessment – Process Assessment	557
<b>Topic 11: Security Information &amp; Event Management</b>	<b>558</b>
Summary	560
<b>Next Topic: Types Of Attacks</b>	<b>561</b>
 <i>Lesson 2 Types Of Attacks</i>	
Agenda	563
<b>Topic 1: Technology-Based</b>	<b>564</b>
DOS/DDOS	565
On-Path Attack	566
DNS Poisoning	567
VLAN Hopping	568
ARP Spoofing	569
Rogue DHCP	570
Rogue Access Point (AP)	571
Evil Twin	572
Password Attacks – Brute-Force	573

Password Attacks – Dictionary	574
MAC Spoofing	575
IP Spoofing	576
Deauthentication	577
Malware	578
Ransomware	579
<b>Topic 2: Technology-Based</b>	<b>580</b>
Phishing	581
Tailgating	582
Piggybacking	583
Shoulder Surfing	584
Summary	585
<b>Next Topic: Network Hardening Techniques</b>	<b>586</b>

<b><i>Lesson 3 Network Hardening Techniques</i></b>	<b>587</b>
Agenda	588
<b>Topic 1: Best Practices</b>	<b>589</b>
Secure Snmp	590
Router Advertisement (RA) Guard	591
Port Security	592
Dynamic Arp Inspection	593
Control Plane Policing	594
Private Vlans	595
Disable Unneeded Switchports	596
Disable Unneeded Network Services	597
Change Default Passwords	598
Password Complexity/Length	599
Enable Dhcp Snooping	600
Change Default Vlan	601
Patch And Firmware Management	602
Access Control List	603

Role-Based Access	604
Firewall Rules	605
<b>Topic 2: Wireless Security</b>	<b>606</b>
Mac Filtering	607
Antenna Placement	608
Power Levels	609
Wireless Client Isolation	610
Guest Network Isolation	611
Preshared Keys (PSKs)	612
EAP	613
Geofencing	614
Captive Portal	615
<b>Topic 3: Lot Access Considerations</b>	<b>616</b>
Summary	618
<b>Next Topic: Remote Access Methods</b>	<b>619</b>

<i><b>Lesson 4 Remote Access Methods</b></i>	<b>620</b>
Agenda	621
<b>Topic 1: Site-To-Site VPN</b>	<b>622</b>
<b>Topic 2: Client-To-Site VPN</b>	<b>624</b>
<b>Topic 3: Remote Desktop Connection</b>	<b>626</b>
<b>Topic 4: Remote Desktop Gateway</b>	<b>628</b>
<b>Topic 5: SSH</b>	<b>630</b>
<b>Topic 6: Virtual Network Computing (VNC)</b>	<b>632</b>
<b>Topic 7: Virtual Desktop</b>	<b>634</b>
<b>Topic 8: Authentication And Authorization Consideration</b>	<b>636</b>
<b>Topic 9: In-Band Vs. Out-Of-Band Management</b>	<b>638</b>
Summary	640
<b>Next Topic: Physical Security</b>	<b>641</b>

<b>Lesson 5 Physical Security</b>	<b>642</b>
Agenda	643
<b>Topic 1: Detection Methods</b>	<b>644</b>
Cameras	645
Motion Detection	646
Asset Tags	647
Tamper Detection	648
<b>Topic 2: Prevention Methods</b>	<b>649</b>
Employee Training	650
Access Control Hardware – Badge Readers	651
Access Control Hardware – Biometric Locks	652
Locking Racks	653
Locking Cabinets	654
Access Control Vestibule	655
Smart Lockers	656
<b>Topic 3: Asset Disposal</b>	<b>657</b>
Factory Reset/Wipe Configuration	658
Sanitize Devices For Disposal	659
Summary	660
<b>Next Topic: Network Troubleshooting Methodology</b>	<b>661</b>

## Module 5

<b>Lesson 1 Network Troubleshooting Methodology</b>	<b>664</b>
Agenda	665
<b>Topic 1: Identify The Problem</b>	<b>666</b>
<b>Topic 2: Establish A Theory</b>	<b>668</b>
<b>Topic 3: Test The Theory</b>	<b>670</b>
<b>Topic 4: Establish A Plan</b>	<b>672</b>
<b>Topic 5: Implement The Solution</b>	<b>674</b>
<b>Topic 6: Verify The Functionality</b>	<b>676</b>
<b>Topic 7: Document The Scenario</b>	<b>678</b>
Summary	680
<b>Next Topic: Troubleshoot Cable Connectivity Issues</b>	<b>681</b>
	681
<b>Lesson 2 Troubleshoot Cable Connectivity Issues</b>	<b>682</b>
Agenda	683
<b>Topic 1: Specifications &amp; Limitations</b>	<b>684</b>
Throughput	685
Speed	686
Throughput	687
<b>Topic 2: Cable Considerations</b>	<b>688</b>
Shielded and Unshielded	689
Plenum and Riser-Rated	690
<b>Topic 3: Cable Application</b>	<b>691</b>
Rollover Cable/Console Cable	692
Crossover Cable	693
Power Over Ethernet	694
<b>Topic 4: Common Issues</b>	<b>695</b>

Attenuation	696
Interference	697
Decibel (DB) Loss	698
Incorrect Pinout	699
Bad Ports	700
Open/Short	701
Light-Emitting Diode (LED) Status Indicators	702
Incorrect Transceivers	703
Duplexing Issues	704
Transmit and Receive (TX/RX) Reversed	705
Dirty Optical Cables	706
<b>Topic 5: Common Tools</b>	<b>707</b>
Cable Crimper	708
Punchdown Tool	709
Tone Generator	710
Loopback Adapter	711
Optical-Time Domain Reflectometer (OTDR)	712
Multimeter	713
Cable Tester	714
Wire Map	715
TAP	716
Fusion Splicer	717
Spectrum Analyzer	718
Snips/Cutters	719
Cable Stripper	720
Fiber Light Meter	721
Summary	722
<b>Next Topic: Network Tools and Commands</b>	<b>723</b>

<b>Lesson 3 Network Tools and Commands</b>	<b>724</b>
Agenda	725
<b>Topic 1: Software Tools</b>	<b>726</b>
Wifi Analyzer	727
Protocol Analyzer/Packet Capture	728
Bandwidth Speed Tester	729
Port Scanner	730
IPERF	731
Netflow Analyzers	732
TFTP Server	733
Terminal Emulator	734
IP Scanner	735
<b>Topic 2: Command Line Tools</b>	<b>736</b>
PING	737
IPCONFIG	739
IFCONFIG	741
IP	742
NSLOOKUP	744
DIG	746
TRACEROUTE	748
TRACERT	749
ARP	750
NETSTAT	752
HOSTNAME	753
ROUTE	754
TELNET	755
TCPDUMP	756
NMAP	757
<b>Topic 3: Basic Network Platform Commands</b>	<b>759</b>
Network Platform Commands	760

Summary	761
<b>Next Topic: Wireless Connectivity Issues</b>	<b>762</b>
<b><i>Lesson 4 Wireless Connectivity Issues</i></b>	<b>763</b>
Agenda	764
<b>Topic 1: Specifications and Limitations</b>	<b>765</b>
Throughput	766
Distance	767
RSSI Signal Strength	768
EIRP Power Rating	769
<b>Topic 2: Considerations</b>	<b>770</b>
Antennas	771
Channel Utilization	772
AP Association Time	773
Site Survey	774
<b>Topic 3: Common Issues</b>	<b>775</b>
Interference	776
Ap Association Time	777
Antenna Cable Attenuation/Signal Loss	778
Rf Attenuation/Signal Loss	779
Wrong SSID	780
Incorrect Passphrase	781
Encryption Protocol Mismatch	782
Insufficient Wireless Coverage	783
Captivate Portal Issues	784
Client Disassociation Issues	785
Summary	786
<b>Next Topic: Troubleshoot General Networking Issues</b>	<b>787</b>

<b>Lesson 5 Troubleshooting Networking Issues</b>	<b>788</b>
Agenda	789
<b>Topic 1: Considerations</b>	<b>790</b>
Device Configuration Review	791
Routing Tables	792
Interface Status	793
Vlan Assignment	794
Network Performance Baselines	795
<b>Topic 2: Common Issues</b>	<b>796</b>
Collisions	797
Broadcast Storm	798
Duplicate MAC Address	799
Duplicate IP Address	800
Multicast Flooding	801
Asymmetrical Routing	802
Switching Loops	803
Routing Loops	804
ROGUE DHCP Server	805
DHCP Scope Exhaustion	806
IP Setting Issues	807
Missing Route	808
Low Optical Link Budget	809
Certificate Issues	810
Hardware Failure	811
Host-Based/Network-Based Firewall Settings	812
Blocked Services, Ports, or Addresses	813
Incorrect VLAN	814
DNS Issues	815
NTP Issues	816

Byod Challenges	817
Licensed Feature Issues	818
Network Performance Issues	819
Summary	820

---

# MODULE 1

---

# Module 1

LESSON 1      OSI MODEL LAYERS AND ENCAPSULATION CONCEPTS

LESSON 2      NETWORK TOPOLOGIES AND NETWORK TYPES

LESSON 3      CABLES AND CONNECTORS

LESSON 4      IP ADDRESSING SCHEMES

LESSON 5      COMMON PORTS AND PROTOCOLS

LESSON 6      NETWORK SERVICES

LESSON 7      CORPORATE AND DATACENTER NETWORK ARCHITECTURE

LESSON 8      CLOUD CONCEPTS AND CONNECTIVITY OPTIONS

Lesson

1

---

# OSI Model Layers and Encapsulation Concepts

- 1 — Welcome to the first lesson of Module 1. In this lesson, you will learn about the:
  - 2 — OSI Model Layers and Encapsulation Concepts.
- 



Network Fundamentals

# AGENDA



OSI Model



Data Encapsulation and Decapsulation



Hi, welcome to COMPTIA Network+ Course

In this lesson, we will talk about:

- OSI Model
- Data Encapsulation and Decapsulation



A professional man with glasses and a beard is sitting at a desk, looking thoughtfully at a computer monitor. The monitor displays a complex data visualization consisting of a bar chart and a line graph. The man is wearing a brown blazer over a blue shirt. The background is slightly blurred, showing an office environment.

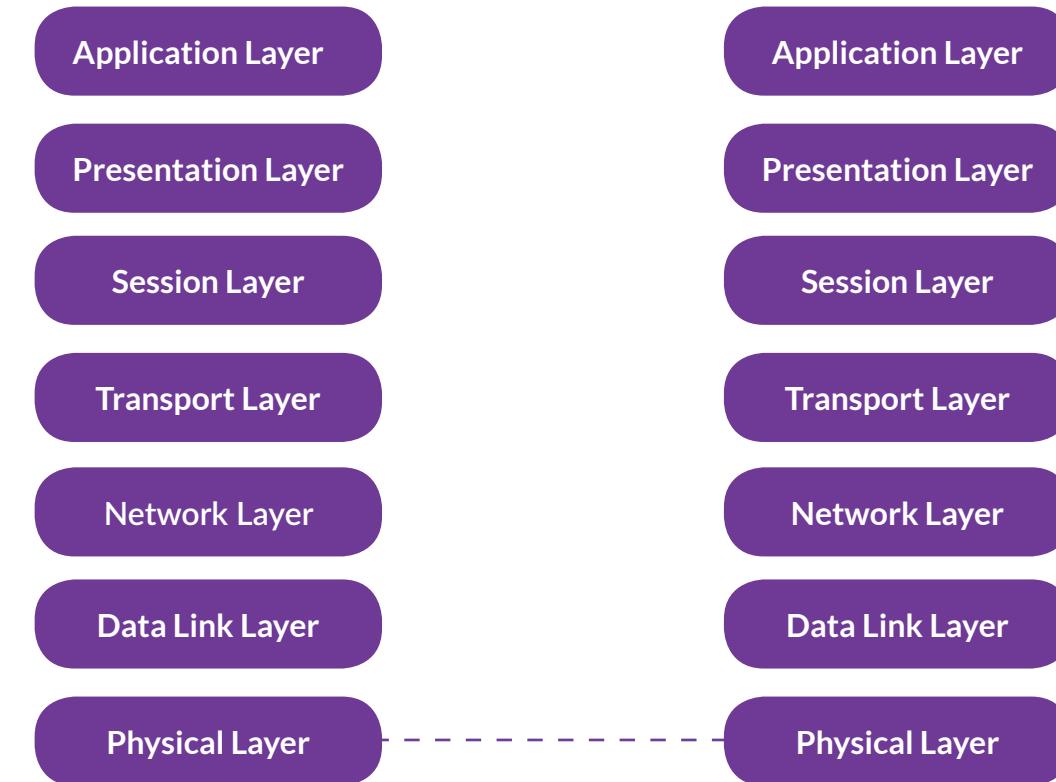
**TOPIC 1**

---

# OSI MODEL LAYERS

---

# Overview



Let's now look at the Open Systems Interconnection (OSI) model, which defines:

- Functions of a networking system
- Characterizes computing functions

Think of two systems communicating with each other – there must be some similarities in the way they communicate, or else they will not be able to. Let's take an example – if one works with the OSI model and another one works with another model, such as TCP/IP, both may not be able to communicate. The OSI model defines the stack of layers, and each layer has a set of responsibilities in network communication. You will get this clarity as you move ahead in this lesson.

For the time being, you should know that there are a total of seven layers, the first one at the bottom, the Physical layer, and then moving to the top to the seventh layer, the Application layer.

# Physical Layer – Layer 1

Application Layer

Presentation Layer

Session Layer

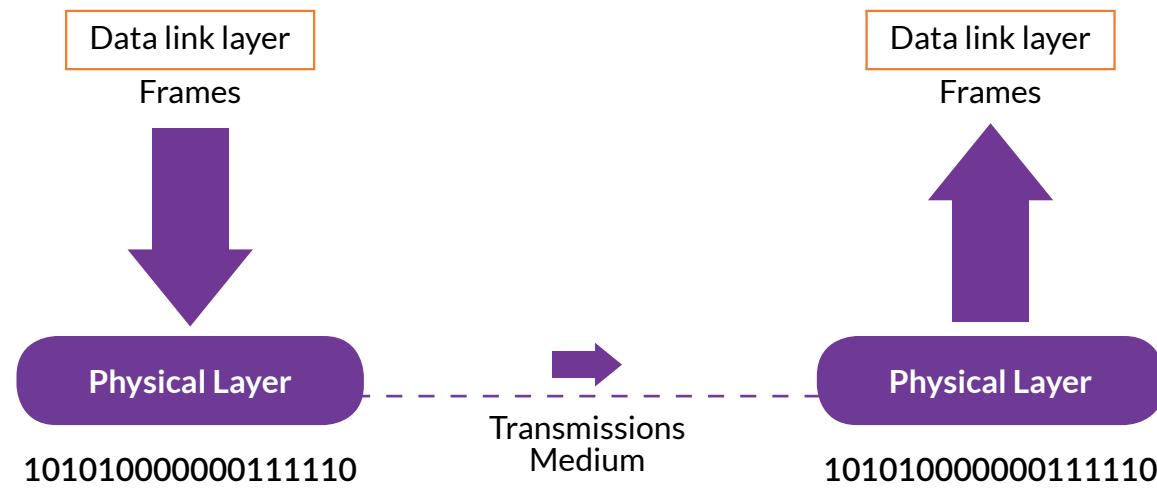
Transport Layer

Network Layer

Data Link Layer

Physical Layer

- In charge of sending digital bits from source to destination device
- Composed of cables, connectors, NIC, repeaters and Hubs
- Does encoding and decoding
- Sends electrical impulses made up of 1s and 0s



Now let's look at the Physical layer of the OSI model. This is the first layer, stacked at the bottom of the OSI model. It has to be present in the source and destination devices during the communication. The source defines triggers the transmission of bits to the destination device.

A system has to work with various physical components, such as cables, network interface cards (NICs), switches, and routers. When a system is connected to a switch via a cable, it can send the bits to the destination system. When the bits, 0 and 1, are sent out by a source system to the destination system, their bits are encoded into electrical signals on a wired network. Instead of electrical signals, the bits are converted into electromagnetic waves on a wireless network.

The Data Link layer is the 2nd layer that passes the information above the layer to the physical layer. We will learn more about it.

# Data Link Layer – Layer 2

Application Layer

- Is responsible for communication between Network and Physical layer.
- Is divided into two sublayers:
  - LLC – Logical Link Control Sublayer
  - MAC Sublayer

Presentation Layer

Session Layer

Transport Layer

Network Layer

**Data Link Layer**

Physical Layer

Layer 2, or the Data Link layer has a key responsibility. It receives the information from the Network layer and passes it to the Physical layer. This is nothing but layer-to-layer communication. One layer sends the information to the next layer. A layer in the OSI model can communicate with the layer above or below it.

When the Data Link layer sends the information, it creates frames and adds physical addresses. The frame that it creates is used to determine the data structure for the network. The Data Link layer comprises two sublayers – Logical Link Control (LLC) and MAC sublayers. Both sublayers play an essential role. The LLC sublayer determines whether the communication is connection-oriented or connectionless. The MAC sublayer contains the MAC address, the physical address of a network interface card, which is eventually used for communication with the other nodes on the networks. Switches use the MAC addresses to locate the destination systems.



# Network Layer – Layer 3

Application Layer

- Receive data from the transport layer and passes it over to the data link layer
- Responsible for:
  - Address conversion
  - Source-to-destination delivery
  - Routing

Presentation Layer

Session Layer

Transport Layer

Network Layer

Data Link Layer

Physical Layer

192.168.100.1

172.16.14.1

192.168.100.1

The Network layer is the mediator of data transmission between the Transport and the Data Link layers. It receives the information from the Transport layer and then passes it to the Data Link layer, which works with the MAC or the physical address unique to every network interface card. On the other side, the Network layer works with the logical addressing, which can be assigned and changed. When you move a laptop or a system from one network to the other network, the system's physical address does not change – unless you change the network interface card. However, the logical address changes. The packet addressing and the conversion of physical to logical addressing occur at the Network layer. No matter which network you are connected to, even though the logical address changes, the physical address remains the same. Then comes the source to destination delivery. The source and destination networks can be different. For example, a system may be sending data to a system on the Internet. The physical address cannot be used in this case, but the logical address is used to find the route to the destination system. The physical addresses are used when the destination system is located on the same network. If it is a different network, then the logical address is used. This is why it is often said to be Layer 3 routing – it allows the different networks to connect. Using the routing, the best path to the destination can also be determined using the routers located on the connected networks.



# Transport Layer – Layer 4

Application Layer

Presentation Layer

Session Layer

**Transport Layer**

Network Layer

Data Link Layer

Physical Layer

- Accepts services from the session layer and passes them to the network layer below.
- Is responsible for:
  - End-to-end message delivery - handles message acknowledgment and traffic control.
  - Error checking - packets arrive without duplication or corruption, and in the correct order
- Contains the TCP and UDP protocols

TCP

UDP

The fourth layer in the OSI model is the Transport layer, which is responsible for:

- Receiving services from the Session layer, which is located above it as the 5th layer
- Provides services to the Network layer, which is located below it as the 3rd layer

The Transport layer performs two essential functions:

End-to-end message delivery - handles message acknowledgment and traffic control.

Error checking - packets arrive without duplication or corruption and in the correct order

A system can be performing several tasks at once. For example, it may be using a Web browser to browse a page on the Internet and copying data from another system on the network. A lot of data packets are arriving at the system. How does the system segregate the data packets and send them to the correct applications, such as a Web browser? In this scenario, the identification of the data packets contains a port number so that the data packets can be sent to the correct application. The data packet differentiation cannot be done with only one IP address because each data packet is meant for the same system that has the same IP address.

The Transport layer is also responsible for ensuring an error-checking method is in place. Its error-checking method ensures:

- Packets arrive in the order they were supposed to arrive in
- There is no duplication of the data packets
- The data packets are not corrupt

The Transport layer contains two key protocols, TCP and UDP. The TCP acronym denotes Transmission Control Protocol. The UDP acronym denotes User Datagram Protocol.



# Session Layer – Layer 5

Application Layer

Presentation Layer

**Session Layer**

Transport Layer

Network Layer

Data Link Layer

Physical Layer

- Manages communication between two devices on a network
  - Regulates the start, continuation, and end of a session
  - Ensures all security concerns are met
  - Manages dialog control, such as:
    - Simplex
    - Half-Duplex
    - Full-Duplex
  - Contains some of the following protocols: NetBIOS, DNS, RPC, and NFS

Now let's look at the OSI model's fifth layer, the session layer, that manages the communication between two devices on a network. It regulates the start, continuation, and end of a session. It performs the following tasks:

Establish a session between two devices

Maintain the session while the communication between the devices is taking place

Terminate the session when the communication between the devices is over

It also regulates the data exchange between two devices. It simply acts as a moderator that determines who can transfer the data and how long the transfer should take place.

It ensures that there is security for the session being established. It also ensures that the security concerns are taken care of. The security can be determined by a login, for example.

It also determines the type of dialog control that will be used. For example, it can be one of the following dialog controls:

- Simplex
- Half-Duplex
- Full-Duplex

Some of the key protocols on this layer are NetBIOS, DNS, RPC, and NFS.



# Presentation Layer – Layer 6

Application Layer

**Presentation Layer**

Session Layer

Transport Layer

Network Layer

Data Link Layer

Physical Layer

- Represents data in a uniform format to an application
- Is also known as the “translation layer”
- Uses methods
  - American Standard Code for Information Interchange - ASCII
  - Extensible Markup Language - XML
- Compresses data for transmission
- Encrypts data for security purposes

The 6th layer or the Presentation layer works according to the name it has been given. It presents the data in a format that is understood by the applications. It formats the data in a uniform format by hiding the differences that the data format differences between two devices that are communicating. The data formatting is performed for the Application layer, the 7th layer of the OSI model. The data received may be different than the Application layer at the receiving system can understand. The Presentation layer formats the data so that the Application layer can comprehend it.

The Presentation layer is also known as the Translation layer because of its capabilities of translating the data from one format to the commonly used format methods, such as:

- American Standard Code for Information Interchange - ASCII
- Extensible Markup Language - XML

Using either of these methods converts the data into 0s and 1s.

It also reduces the number of bits transmitted on the network by applying compression to the data. It also encrypts the data for security purposes.

# Application Layer – Layer 7

## Application Layer

## Presentation Layer

## Session Layer

## Transport Layer

## Network Layer

## Data Link Layer

## Physical Layer

- Is the layer where the user interacts with the devices
- Serves as an interface for the applications, such as:
  - Email applications
  - Web browsers
- Example of protocols running on Layer 7:
  - FTP
  - DHCP
  - DNS
  - SMTP
  - HTTP

The Application layer is the OSI model's final layer, the 7th layer. It serves as the interface for users and application processes to access network services. Using the Application layer, the users can communicate with the applications.

Let's see how it works. The Application layer allows the users to work or interact with the applications installed on a system. When a user interacts, the data is passed on to the user in a standard format. Even if the user accesses the application from a different network, the data is still standardized for presentation.

The following protocols exist on the Application layer:

- File Transfer Protocol (FTP)
- Dynamic Host Configuration Protocol (DHCP)
- Domain Name System (DNS)
- Simple Mail Transfer Protocol (SMTP)
- Hypertext Transfer Protocol (HTTP)

These protocols are discussed in the upcoming lessons in Module 1.



## *TOPIC 2*

---

# ENCAPSULATION & DECAPSULATION

---

# Ethernet Header

Field Length(Bytes)	Preamble	Destination MAC Address	Source MAC Address	Length	Payload	FCS
Field Length(Bytes)	8	6	6	2	46-1500	4

A network is created so that communication between the devices can take place. The communication between two devices is done in a format known as frames, which contains the information that needs to be transferred from the source to the destination system. The Ethernet network, on which the communication needs to occur, creates frames by dividing the information.

Now the question is what precisely a frame is? Overall, a frame comprises the following pieces:

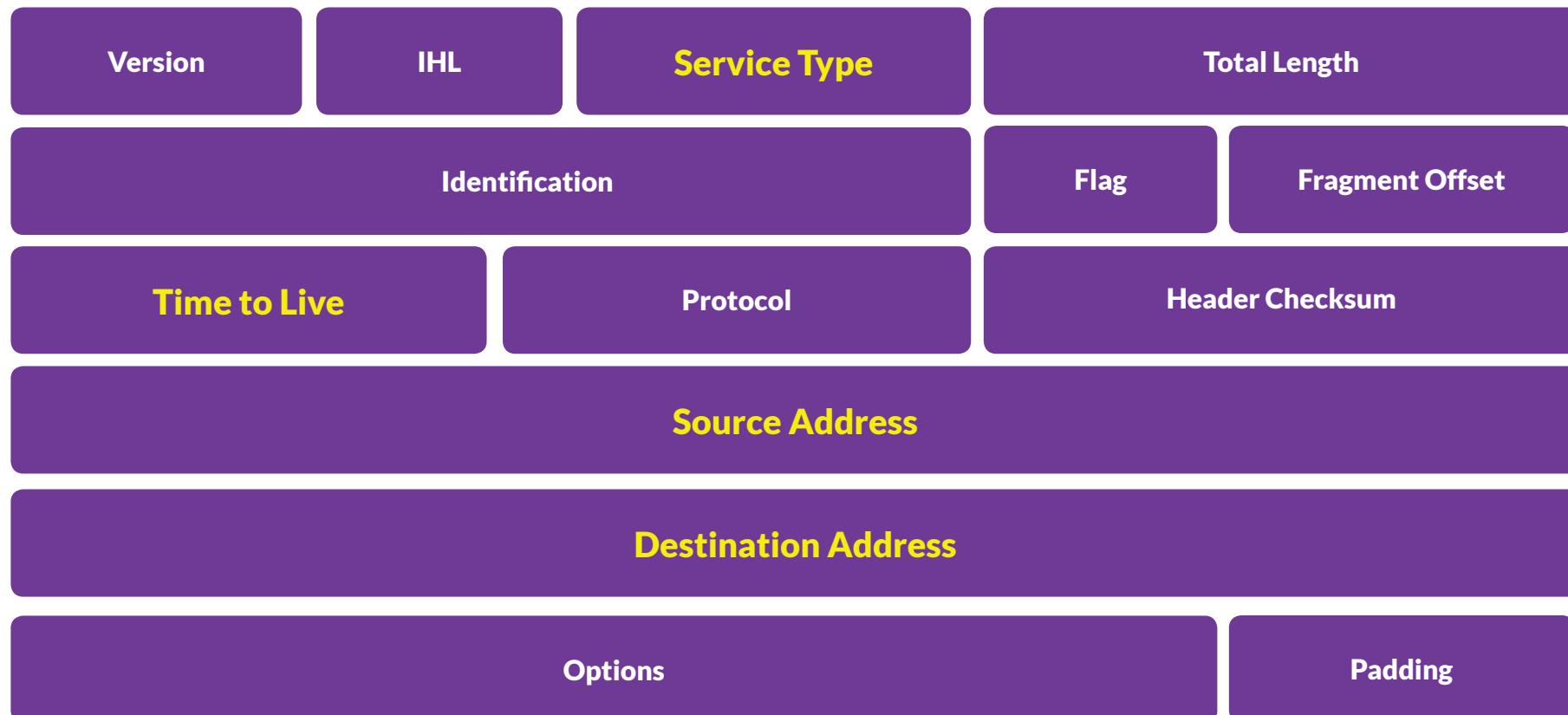
- Information about the header and trailer of the transmission
- The data that needs to be transmitted

If you break down a frame, it contains several fields, as shown in the slide. These fields are:

- Preamble: consists of 8 bytes (including 1 byte of Start of Frame delimiter). The preamble consists of seven bytes. It is mainly used to establish synchronization between the sending and receiving devices. It uses the alternating 1s and 0s.
- Destination Address (DA): contains the physical or the MAC address of the recipient system.
- Source Address (SA): contains the physical or the MAC address of the sending system.
- Length: is a 2-byte long field that determines the length of the Ethernet frame. Even though this field can hold the length 0 to 65534, its length is restricted to a maximum of 1500 due to limitations in Ethernet.
- Payload: contains the actual data. It can have a minimum length of 46 bytes and a maximum length of 1500 bytes. If the length is shorter than 46 bytes, extra 0s are added to meet the minimum length.
- FCS: Is the Frame Check Sequence (FCS) that uses the cyclic redundancy check (CRC) to the field includes a checking mechanism to ensure that the frame is without any corruption. It contains a 32-bit hash value generated based on Destination Address, Source Address, Length, and Data fields.



# IP Header



# IP Header

Each frame transmitted over the Ethernet v4 network contains an IP header, which contains static and dynamic values. It contains static values like the IP version. Yet, it also contains dynamic values, such as Time to Live (TTL), that are changed or modified while the frame is in transit. To understand the IPv4 header better, you need to know some of the required fields it contains. These fields are:

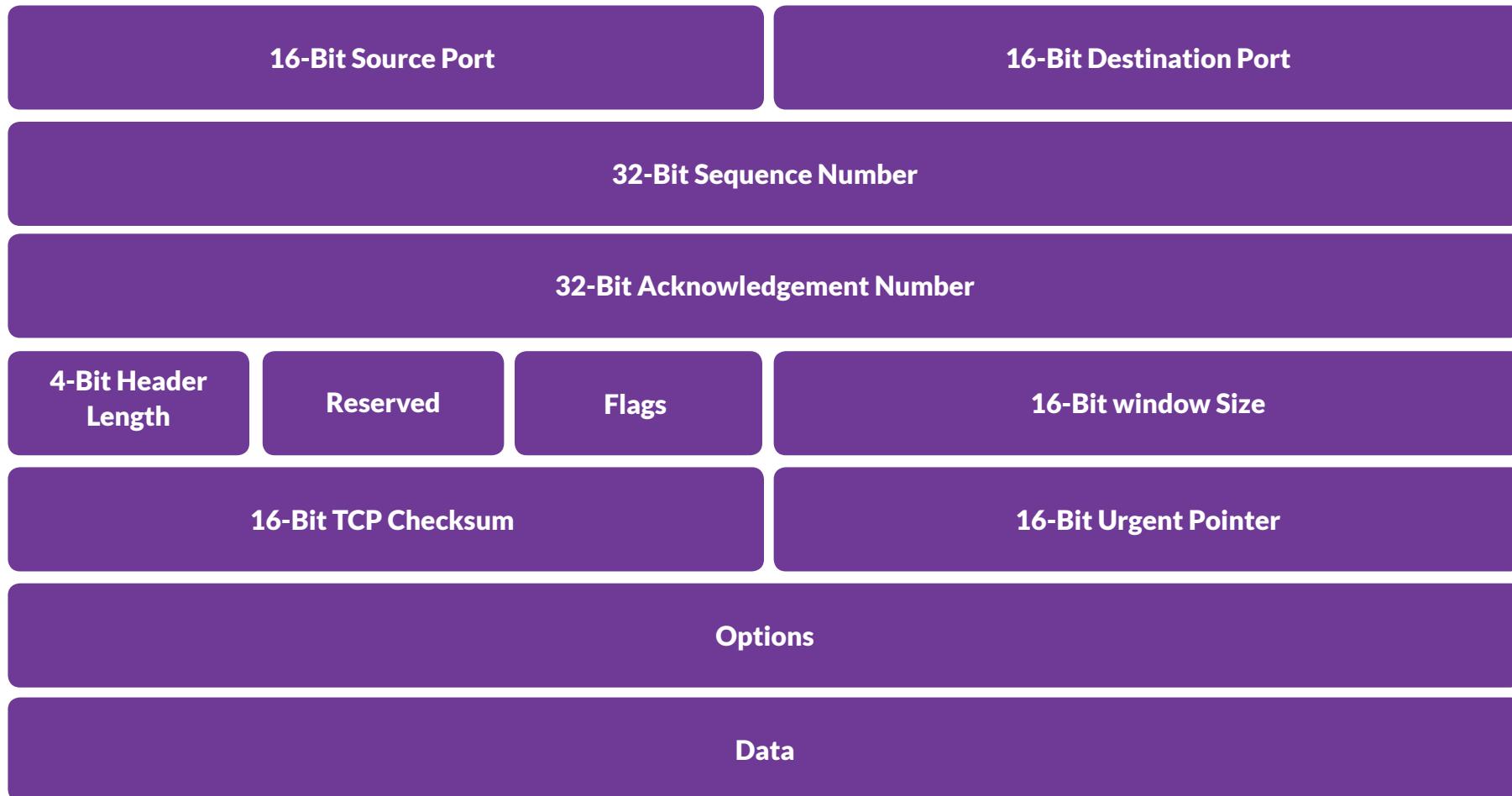
- Service type: Has the quality-of-service information
- TTL: defines how long the packet is going to live
- Source address: contains the IPv4 address of the system that is sending the information
- Destination address: contains the IPv4 address of the system that is receiving the information

Other than the key fields, there are several fields, which are:

- Version: defines the IP version, such as IPv4
- IHL: stands for Internet Header Length (IHL) that describes the header's length
- Total Length: describes the total length of a packet that includes the header and data
- Identification: is used for unique fragment identification
- Flag: is used to set control flags for fragmentation
- Fragment Offset: defines where a specific fragment belongs
- Protocol: indicates the upper-layer protocol used in the data portion
- Header Checksum: Used for header error detection
- Options: contains various optional parameters
- Padding: is used for padding extra values to make it 32-bit



# TCP Headers



# TCP Headers

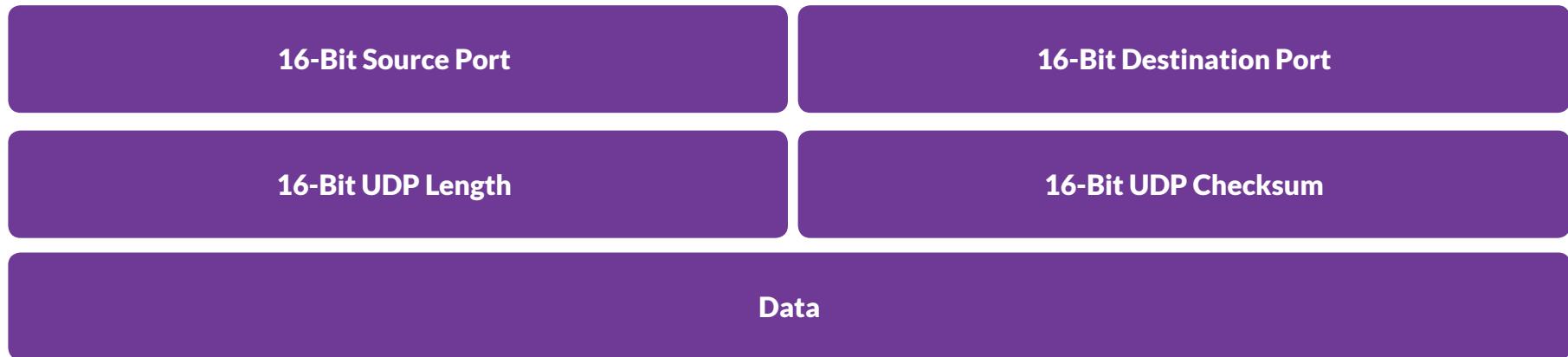
TCP resides at the OSI model's layer 4, the Transport layer. TCP is a connection-oriented protocol. It has several fields, such as

- Source Port: is a 16-bit field that defines the sender's port number
- Destination Port: is a 16-bit field that defines the receiver's port number
- Sequence Number: is a 32-bit field that defines the amount of data sent
- Acknowledgment Number: is a 32-bit field that is used by the receiver to request for the next TCP segment
- Header Length: is a 4-bit field that defines the header's length
- Reserved: is a 3-bit unused field that is always set to 0
- Flags: is a 9-bit control bits field used to establish and terminate connections. These flags are Nonce Sum (NS), Congestion Window Reduced (CWR), Explicit Congestion Notification Echo (ECE), Urgent (URG), Acknowledgment (ACK), Push (PSH), Reset (RST), Synchronize (SYN), and Finish (FIN).
- Window size: is a 16-bit field that defines the number of bytes a receiver can receive
- Checksum: is a 16-bit field that contains a checksum to ensure the TCP header is not corrupted or manipulated
- Urgent Pointer: is a 16-bit field that determines the last urgent data byte
- Options: can be of 0 to 320-bits to define the ending point for urgent data

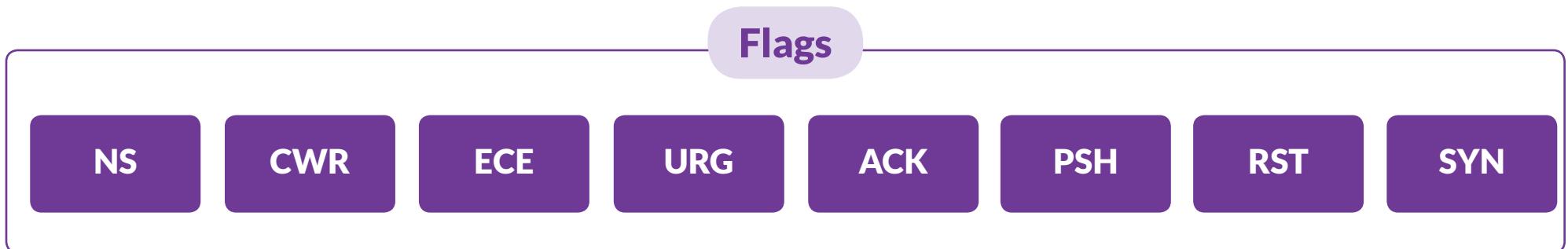
Data: is upper-layer protocol (ULP) data that varies in size



# UDP Headers



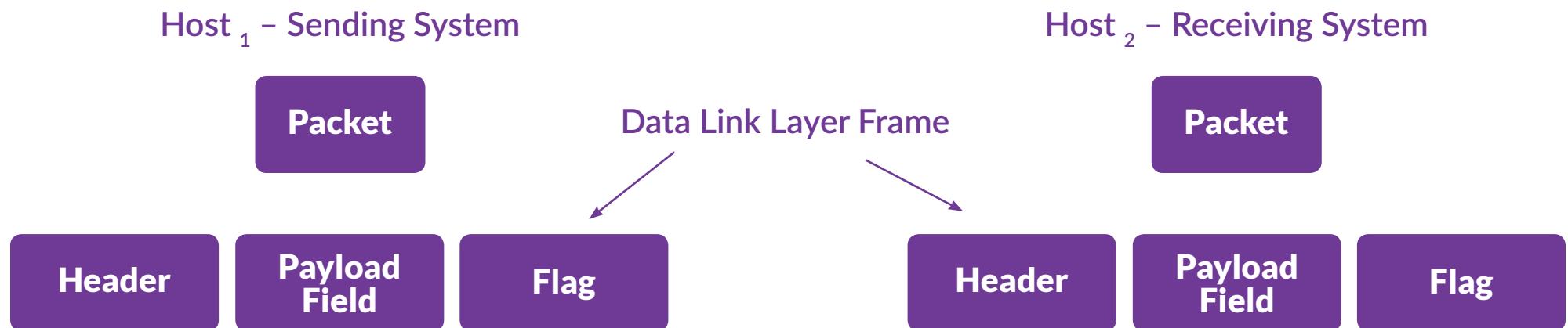
# TCP Flags



TCP Flags or control bits is a 9-bit field that contains the following flags:

- Nonce Sum (NS): is a flag that protects against malicious concealment of packets from a sender
- Congestion Window Reduced (CWR): is an acknowledgment that confirms that congestion-indication echoing is received
- Explicit Congestion Notification Echo (ECE): is a flag that indicates congestion
- Urgent (URG): is a pointer that indicates that the data with this pointer needs to be given higher priority over other data
- Acknowledgment (ACK): is used for acknowledgment
- Push (PSH): is a flag that mandates an application to send data immediately without waiting for the entire TCP segment.
- Reset (RST): requires the connection to be terminated
- Synchronize (SYN): is used for the initial three-way handshake and set the sequence number

# Payloads



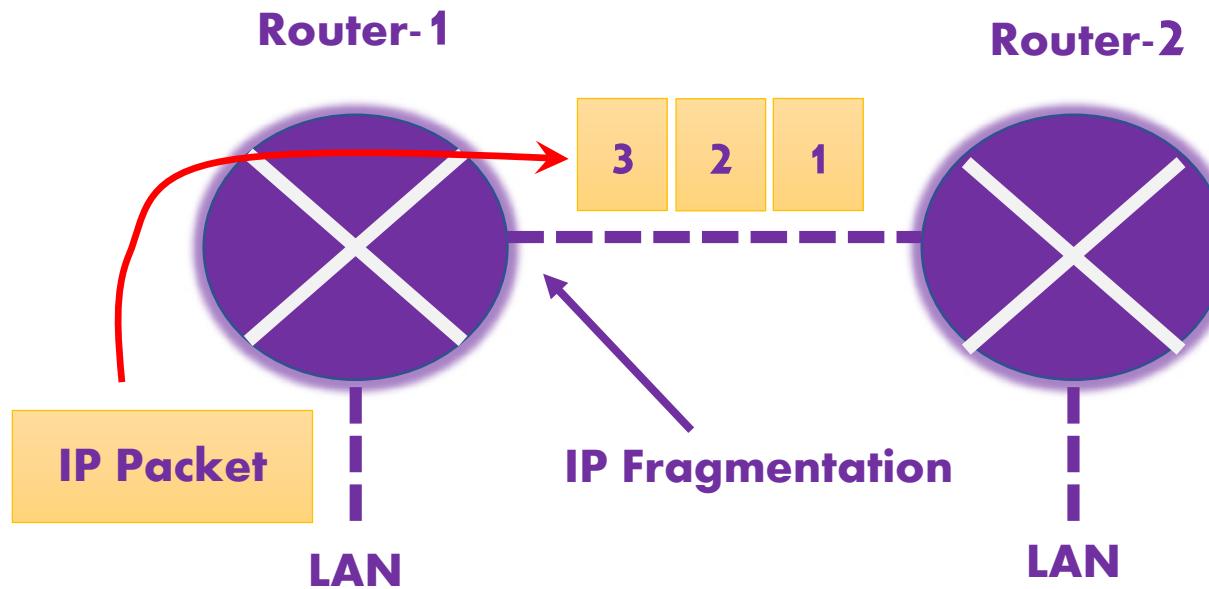
Consider the amount of data being transmitted to a destination host. The amount of data in this scenario is the payload. When data is being sent, it contains the header, payload field, and flags if required. When you send the data, these fields will be present. When the receiving side receives it, it uses its OSI layers to process the data, starting at the Application layer to the lower order.

Payloads are of two types:

- Fixed: the data being transmitted is in a fixed size. Every frame carries the same set of data.
- Variable Length: the amount of data being transmitted is variable. Each frame can carry a different amount of data.

# MTU

- Is the largest maximum frame or packet for given network
- If the IP packet is larger than the MTU, the router breaks packets into smaller packets using a process called IP Fragmentation



# Summary



OSI Model



Data Encapsulation and Decapsulation



That's the end of the lesson.

Here we covered:

- OSI Model
- Data Encapsulation and Decapsulation

*NEXT TOPIC*

---

# NETWORK TOPOLOGIES AND NETWORK TYPES

---

Lesson

2

# Network Topologies and **Network Types**

- 1 — Welcome to the lesson 2 of Module 1. In this lesson, you will learn about the:
- 2 — Network topologies and network types. So, let's get started.



Network Fundamentals

# AGENDA



Mesh



Star/hub-and-spoke



Bus



Ring



Hybrid



Network types and characteristics



Service-related entry point



Virtual network concepts



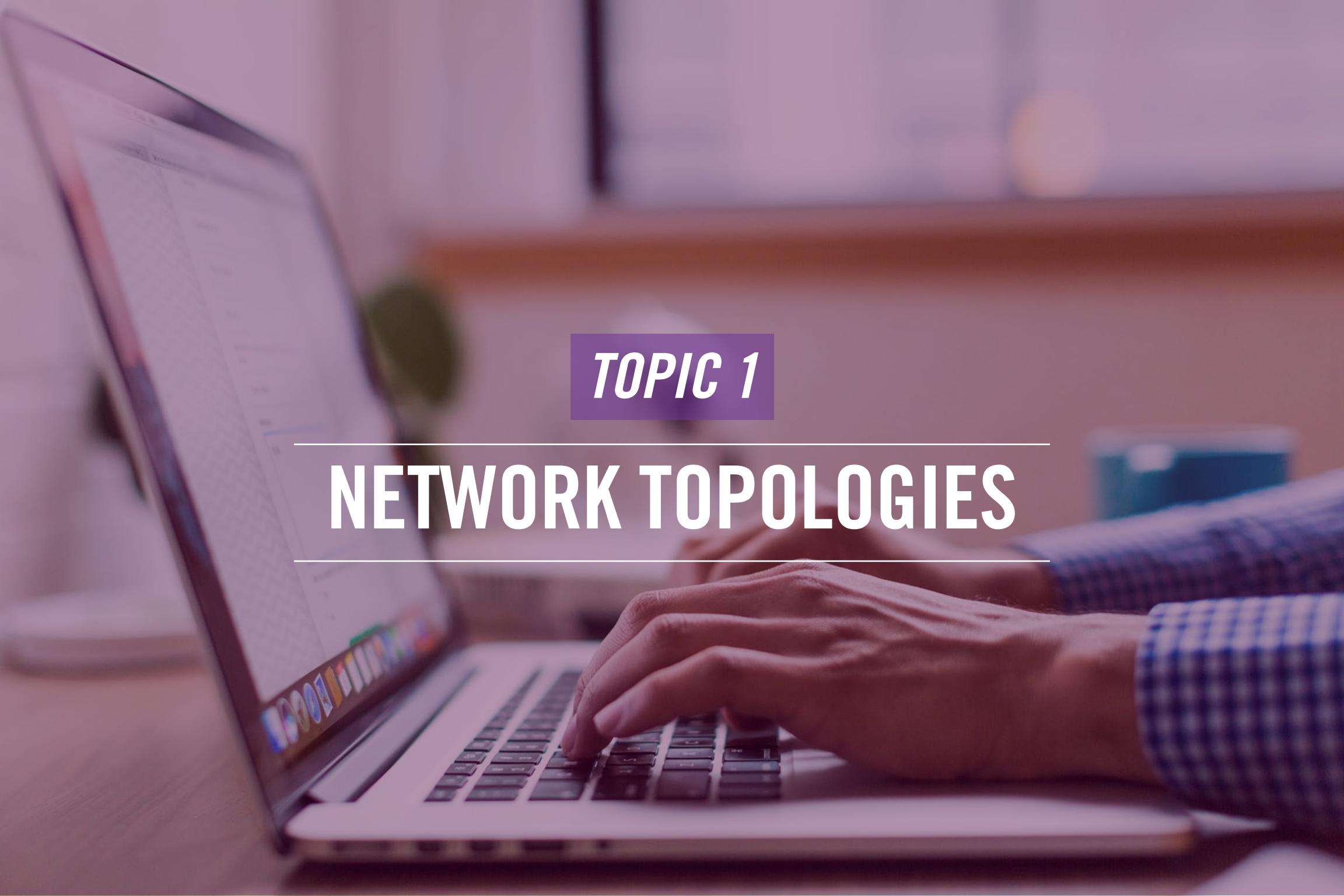
Provider links



Hi, welcome to COMPTIA Network+ Course In this lesson, we will talk about:

- Mesh
  - Star/hub-and-spoke
  - Bus
  - Ring
  - Hybrid
- Network types and characteristics
  - Service-related entry point
  - Virtual network concepts
  - Provider links



A photograph of a person's hands typing on a laptop keyboard. The laptop screen shows a blurred interface, possibly a spreadsheet or database. The background is a wooden desk with some papers and a small potted plant.

*TOPIC 1*

---

# NETWORK TOPOLOGIES

---

# Mesh

Hybrid

Ring

Bus

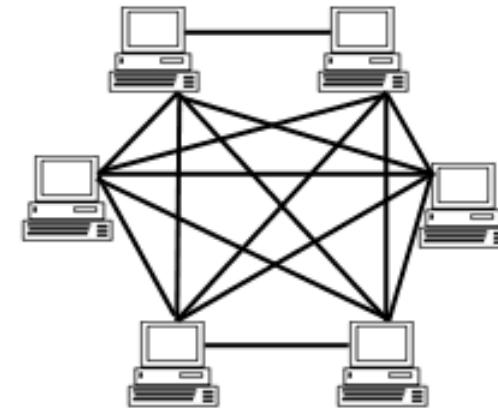
Star/Hub & Spoke

Mesh

- Has each node connecting to the other nodes
- Can be:
  - Full Mesh
  - Half Mesh

[What is Mesh Topology?  
\(computerhope.com\)](#)

## Mesh Topology



ComputerHope.com

You can have from a few to hundreds of nodes on a network. In the mesh topology, each node is connected to the other node on the network. In this way, each node has several paths to transmit data. If one of the paths is unavailable, the data can be transmitted through different paths. The unavailability of one node does not impact the rest of the network. Similarly, you can add or remove a node without impacting the rest of the network.

A mesh network can either be full mesh or half mesh. In a full mesh network, each node is connected to the other nodes in the network. You can calculate the number of nodes with the given formula:

$$n(n-1)/2$$

For example, if you have 10 nodes, the formula will work in the following manner:

$$10(10-1)/2 = 10(9)2 = 90/2 = 45$$

So, each node will have 45 connections.

In the half mesh, the node is connected to a minimum of two nodes. If one node fails, the network continues to function without being impacted.

# Star/Hub and Spoke

Hybrid

Ring

Bus

**Star/Hub & Spoke**

Mesh

- Is used in most networks today
- Requires a centralized switch to which the devices connect
- Helps in centralized network management
- Provides the ease of adding or removing devices

[What is Star Topology?](#)  
[computerhope.com](http://computerhope.com)



When your devices are connected to a switch, they form a star topology. The switch is a centralized device that connects all other nodes. The star topology is the most used in today's world.

With the star topology, the network management is centralized. You can easily add or remove devices without impacting the rest of the network. Even if a node fails, it does not impact the rest of the network. However, if the centralized switch or the device goes down, the entire network goes down.

# Bus

Hybrid

Ring

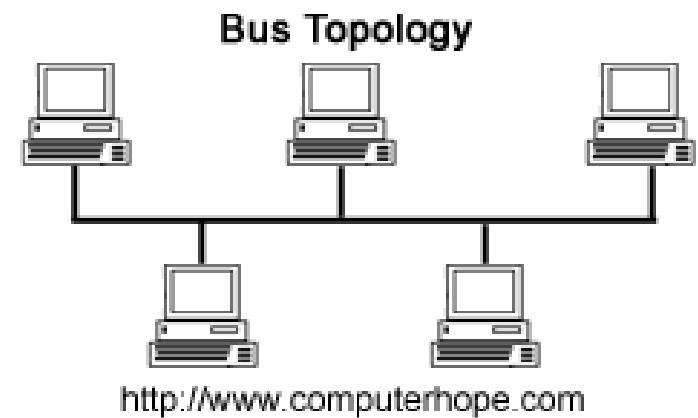
Bus

Star/Hub & Spoke

Mesh

- Has a single backbone to which the devices connect
- Is mainly used in small networks
- Is difficult to troubleshoot and add more devices

[What is Bus Topology?](#)  
[\(computerhope.com\)](http://www.computerhope.com)



The bus topology works with a single backbone to which all the devices are connected. Each of the devices is directly connected to the backbone. If the backbone is broken or split, the network is divided into two parts or fails. The bus topology works well in the smaller networks. However, it is difficult to troubleshoot an issue if the network is down.



# Ring

Hybrid

Ring

Bus

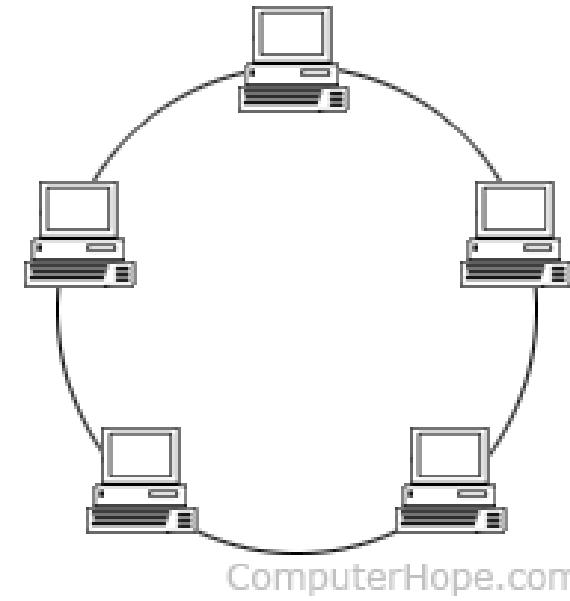
Star/Hub & Spoke

Mesh

- Connects the devices in a loop or circular fashion
- Requires the data to travel from one device to another
- Is affected if one device goes down

[What is a Ring Topology?](#)  
[computerhope.com](http://computerhope.com)

## Ring Topology



All nodes in a ring topology are connected in a loop or circular fashion. Each node connects to two nodes – one in front and one in back. The data sent from one node needs to travel from one node to the next until it reaches its destination. The data travels in a single direction, which means that the ring topology is considered a unidirectional network.

If one node or device goes down, the entire network is impacted.

# Hybrid

## Hybrid

Ring

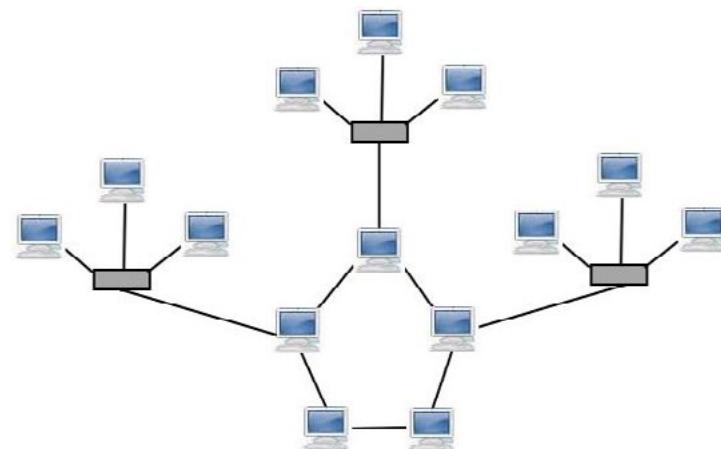
Bus

Star/Hub & Spoke

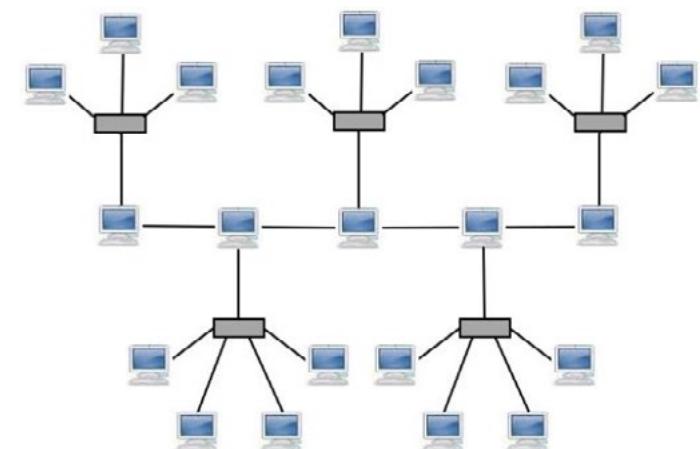
Mesh

- Combines two or more network topologies

Star-Ring hybrid topology



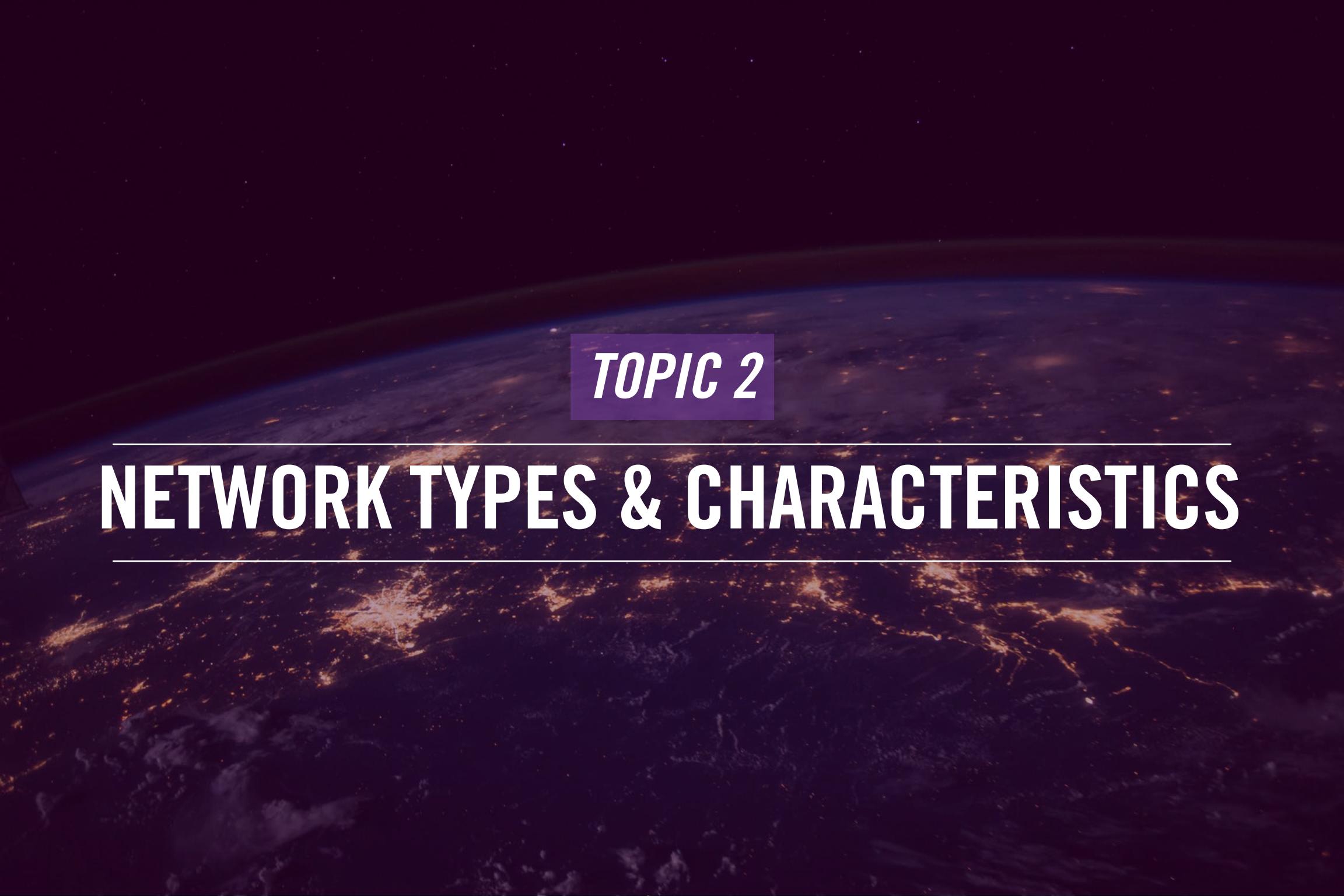
Star-Bus hybrid topology



[What is Hybrid Topology? \(computerhope.com\)](http://computerhope.com)

A hybrid topology is formed when you combine two different topologies. You can mix and match topologies, such as bus, mesh, star, and ring. Whether or not you choose to implement hybrid topology depends on your business needs and requirements.

For example, you can have a Star-Ring topology to mix both star and ring topologies. Another example can be a Star-Bus topology in which you mix both bus and star topologies.

The background of the slide is a dark, aerial photograph of a city at night. The city lights are visible as small, glowing yellow and white dots scattered across the landscape. In the distance, a bright horizon line suggests the presence of the sun or moon. The overall atmosphere is mysterious and futuristic.

## *TOPIC 2*

---

# NETWORK TYPES & CHARACTERISTICS

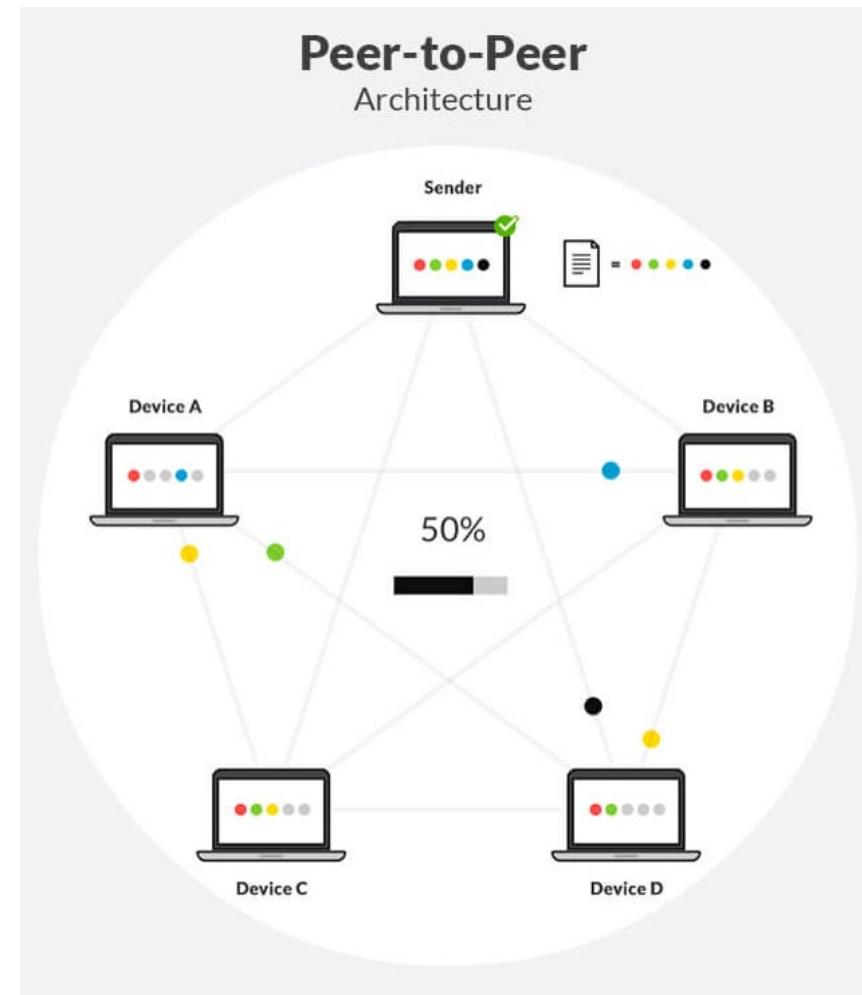
---

# Peer-to-peer

- Connects devices without any centralized controlling authority
- Considers every device with same privileges
- Treats every device as a peer to other devices
- Works well with the smaller networks

[What's the difference between peer-to-peer \(P2P\) networks and client-server? | Resilio Blog](#)

Have you ever connected two nodes without using a switch or a hub? If yes, that is the peer-to-peer network you have formed. There is no centralized device through which the traffic is routed in a peer-to-peer network. Every node in the peer-to-peer network is equal to the remaining nodes. Each node can act as a client and a server to another node. For example, if a client is accessing an application or data from another node is considered to be a client node. At the same time, the same node can be providing some services to another node. In this scenario, it is acting as a server node. There is less security in the peer-to-peer network as each node is responsible for its security. The peer-to-peer network works well when there are a few nodes.



# Client-Server

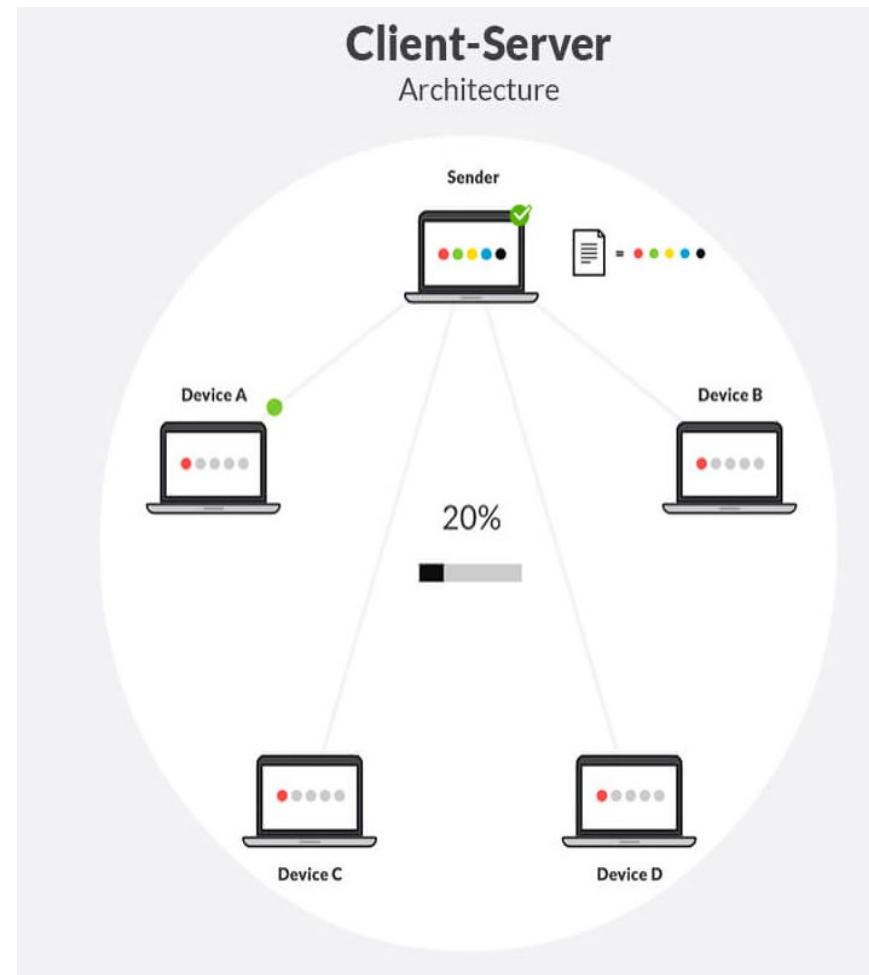
- Assigns the control to a centralized authority
- Is designed to keep server as the controlling authority
- Can be used for various purposes, such as authentication
- Is unavailable when the server goes down

[What's the difference between peer-to-peer \(P2P\) networks and client-server? | Resilio Blog](#)

Remember, the peer-to-peer network did not have any centralized device to route information. Each node was directly talking to another node. There is a centralized authority in the client/server network that controls the network. For example, a domain controller is a server in a Windows domain, and all Windows systems are clients. So, there is one server and several clients in most cases.

The centralized server, such as the domain controller, controls the clients. For example, it has several rolled-out policies for the clients. It has centralized authentication control – all clients authenticate with the domain controller.

If the centralized server goes down, it impacts the network.



# Peer-to-peer

	LAN	MAN	WAN
Acronym Expansion	Local Area Network	Metropolitan Area Network	Wide Area Network
Area Coverage	Building or campus	City	Country or countries, continents
Ownership	Private	Private, Public	Private, Public
Speed	High	Medium	Slow
Congestion	Low	Medium	High

LAN or Local Area Network is a network that connects various devices and systems within a building. You may also have various systems connected at home using a hub. If you have, then it is a LAN. It has various characteristics, like a private network that offers high speed. Typically, if you segment the network properly, it has low congestion.

MAN or Metropolitan Area Network is an extended version of LAN that spans over a city or a metropolitan area. It can be public or private. For example, an organization has various branch offices all over the city. It can set up a private MAN instead of a LAN. It offers a slower speed than LAN. It also offers higher congestion than LAN. WAN or Wide Area Network is a network that spans over a country or countries, or even continents. It can be public or private. It can be owned by an organization that has a presence in several countries. The Internet can be considered as a public WAN. Due to several hops, it has slow speed and a high congestion level.



# Wireless Local Area Network (WLAN)

- Is a wireless network with several devices connected to it
- Works just like a wired Ethernet network
- Is usually configured in home or offices
- Can be configured in two modes:
  - Infrastructure
  - Peer-to-peer (Independent)

## [WLAN \(Wireless Local Area Network\) Definition](#) [\(techterms.com\)](#)

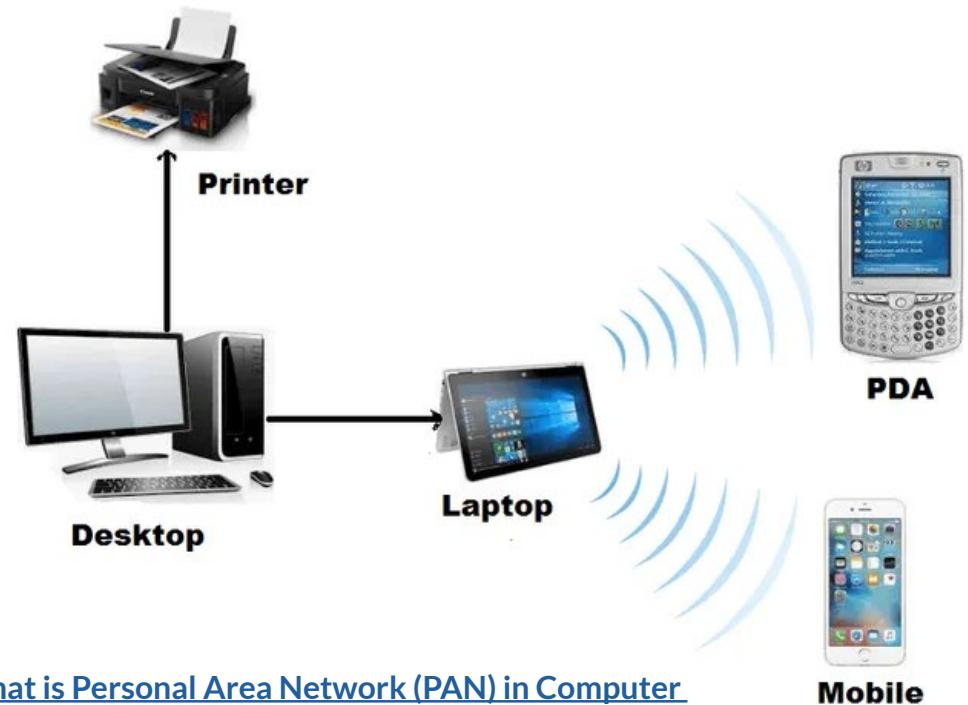
WLAN or Wireless Local Area Network is like the wired LAN. Instead of the wired device, here wireless connectivity is used. Devices or systems like laptops with wireless capability can connect to the wireless network. You would often find wireless networks in homes, offices, cafes, hotels, and even airports. It provides the flexibility for the users to connect to the network while they are on the move.

A wireless network can be configured either using infrastructure or the peer-to-peer network. The infrastructure mode requires you to have a wireless access point. The infrastructure mode can further be configured to use either a password or an authentication server, such as a RADIUS server. For example, if you configure a hot spot on one mobile and connect to another mobile, it is a peer-to-peer wireless network.



# Personal Area Network (PAN)

- Is a single user environment with several devices
- Connects various devices, such as:
  - System
  - Gaming console
  - Mobile
  - Tablet
  - Printer
- Is limited within 10 meters
- Can be combination of wired and wireless network



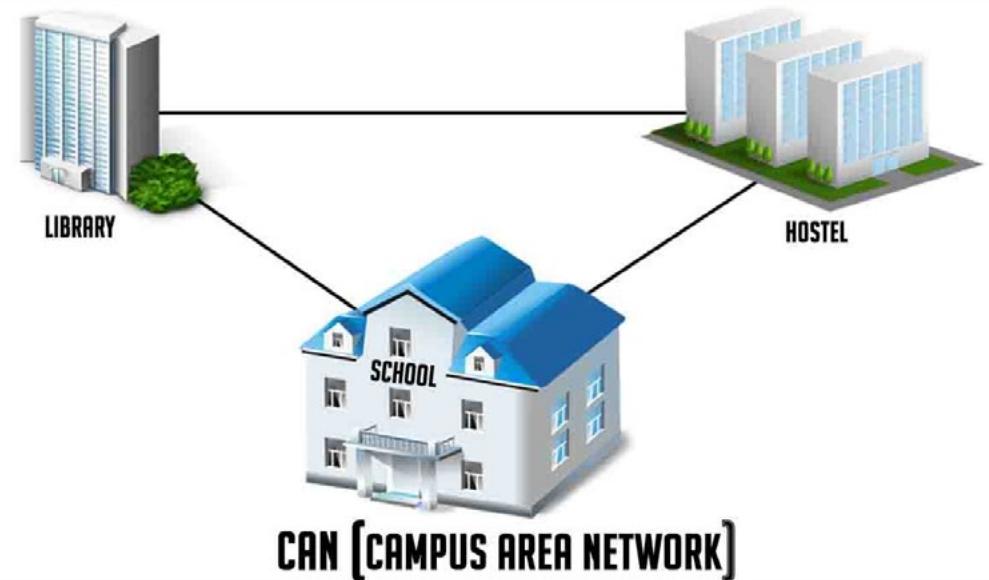
[What is Personal Area Network \(PAN\) in Computer Networking? Examples \(digitalthinkerhelp.com\)](http://digitalthinkerhelp.com)

A Personal Area Network or PAN is a single-user environment with several devices connected to a system. PAN is usually found at homes where users connect multiple devices, such as a printer, mobile, game consoles, and tablets, to a single system.

PAN has distance limitations dependent on the length of the wires used to connect devices with the systems. You can have wired and wireless devices, which are also limited within the range of wireless connectivity.

# Campus Area Network (CAN)

- Is a network within a university or college
- Interconnects various LANs from different buildings
- Is larger than LAN but smaller than MAN
- Can be a combination of wired and wireless network

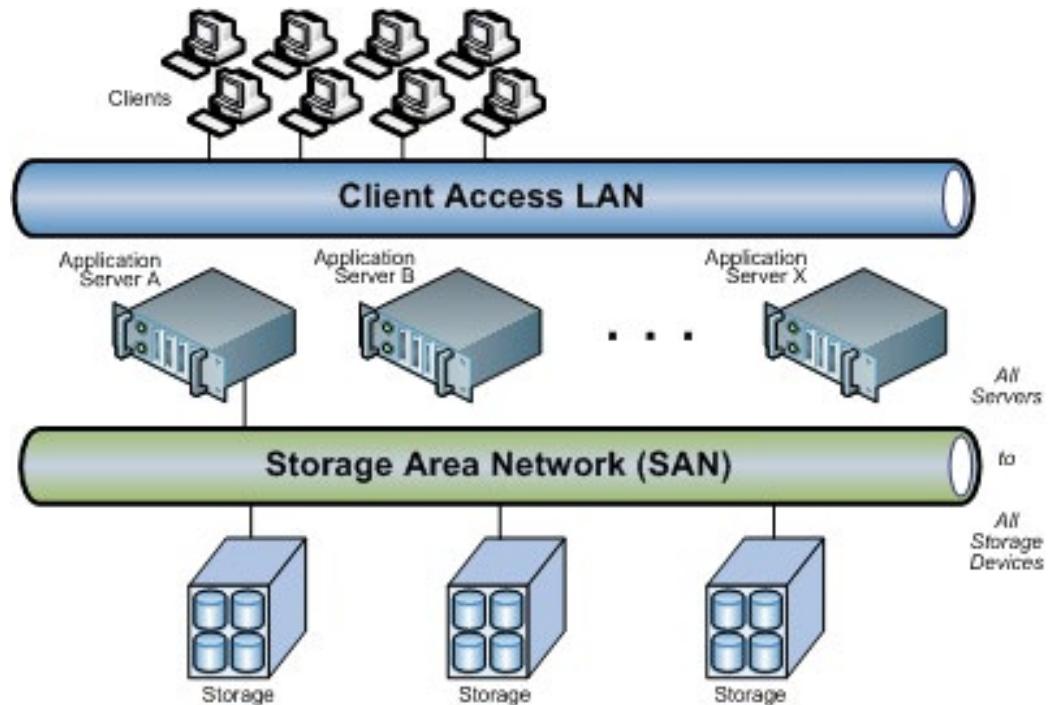


If you have ever been to a university or college, they have their network known as Campus Area Network (CAN). A college or university consists of several buildings that run this network. Unlike LAN, which is limited to a single building, CAN spreads out to several buildings within the college or university campus. Like PAN, CAN work with the combination of wired and wireless or either one of them.

[What is a Campus area network \(CAN\) with an example - IT Release](#)

# Storage Area Network (SAN)

- Is designed for the storage systems
- Segregates the traffic from typical LAN traffic
- Is designed within the datacenter
- Uses protocols, such as Fiber Channel and iSCSI
- Helps to increase storage utilization and security



## What Is a Storage Area Network (SAN)? | SNIA

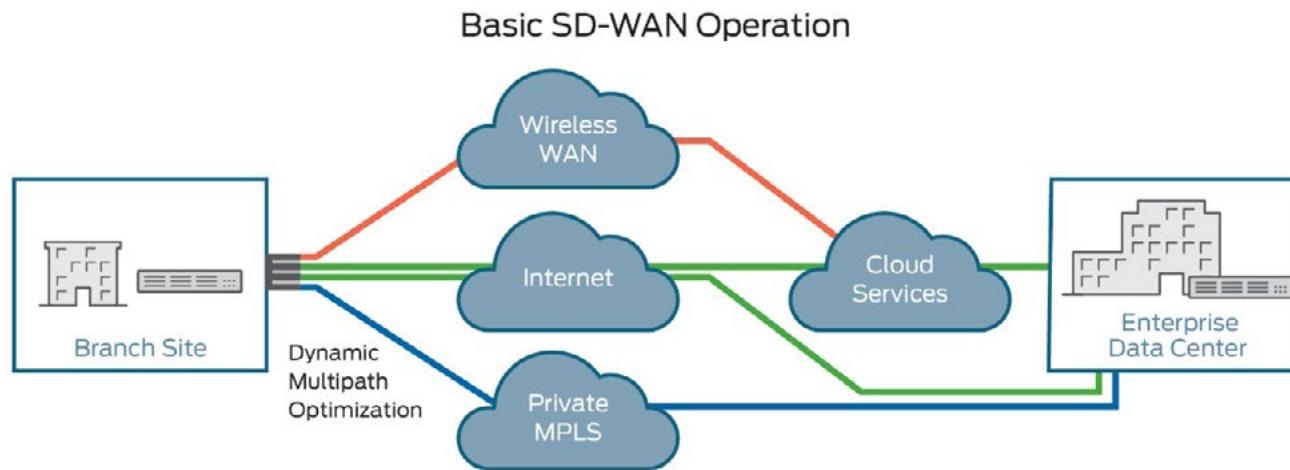
One of the critical differences between LAN and SAN is that hosts storage-related hardware, such as switches and storage devices. On a LAN, you have systems and servers. On a Storage Area Network or SAN, you have storage systems. Unlike LAN, a SAN can span across several sites.

The key intent of a SAN is to segregate the storage traffic from the regular network traffic. SAN is designed within a datacenter but segregated from the normal LAN. You would have a SAN designed to use Fibre Channel technology using Fibre Channel Protocol (FCP). SAN can also use Fibre Channel over Ethernet (FCoE) to the high-speed transmission of the storage traffic over the Ethernet network. Another protocol that can be used is iSCSI.

The key reasons for using a SAN are for high-speed transmission of storage traffic, increasing storage utilization by having everything in a single box designed specifically for storage, and increased security.

# Software-defined Wide Area Network

- Is a WAN architecture that uses software to manage devices
  - Integrates various protocols, such as MPLS and LTE
  - Can make real-time changes without impacting the existing functionality



What is SD-WAN (Software-Defined Wide-Area Network)? | Juniper Networks

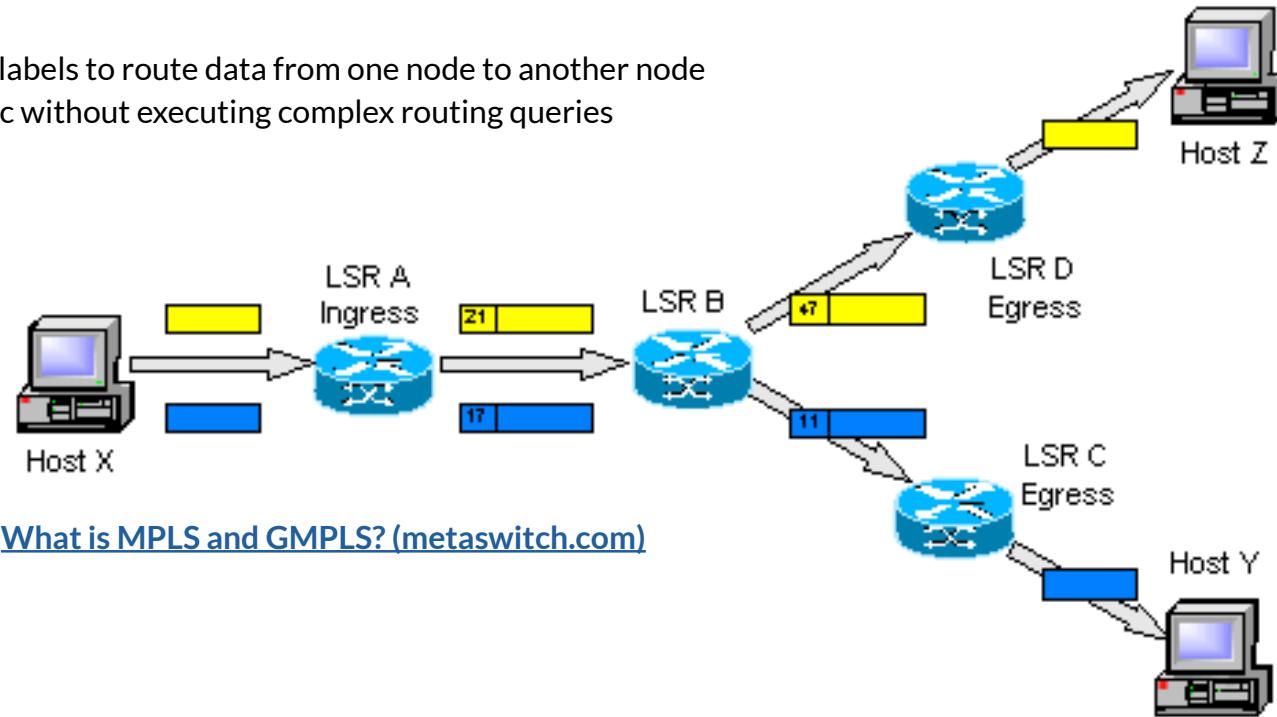
In a typical WAN scenario, you have to manage your devices individually. For example, you would manage several routers individually. With the Software-defined Wide Area Network (SDWAN), the scenario changes slightly. You use software to manage your devices and services running over the WAN.

With the SDWAN, you can use different transport protocols, such as MPLS or LTE. MPLS stands for Multiprotocol Label Switching, and LTE stands for Long-Term Evolution.

With the existing devices and services running, you can make changes to them without taking them offline. This is because SDWAN decouples the underlying hardware from its control methods. You can add any hardware and manage it without adding more complexity to the architecture.

# Multiprotocol Label Switching (MPLS)

- Is a WAN protocol that uses labels to route data from one node to another node
- Speeds up the network traffic without executing complex routing queries



In the previous slide, you learned about MPLS, Multiprotocol Label Switching, as a transport protocol in SDWAN. Let's understand what MPLS is. A WAN protocol uses labels to route data from one node to another node. Labels are nothing but numbers assigned to the data that needs to be transported. The labels are assigned in the data headers and then forwarded to the destination as required. The labels are then used to forward data.

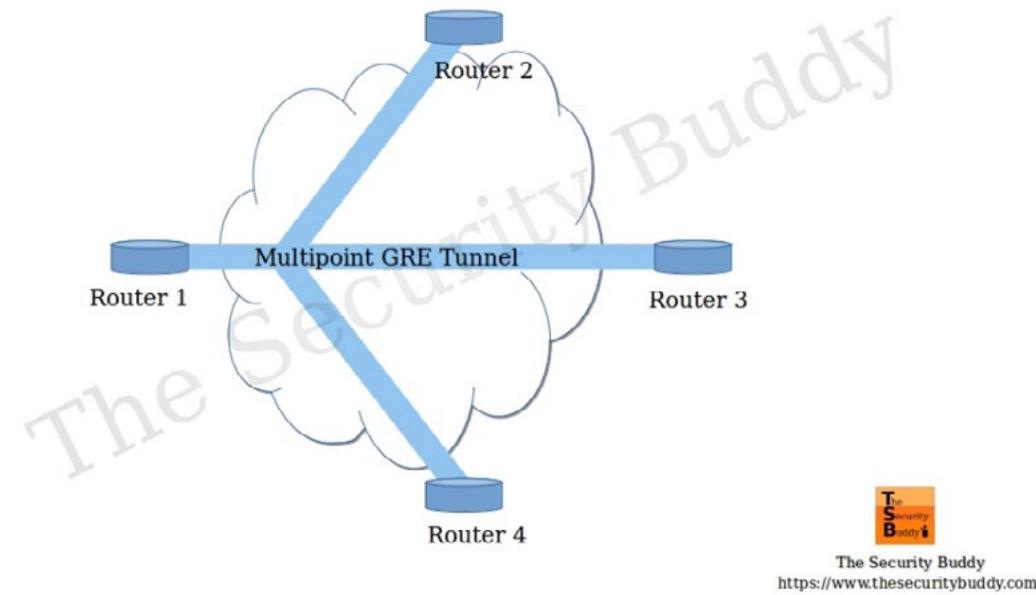
With the use of labels, data prioritization can also be done. For example, voice and video data are assigned a higher priority than regular data. There are different types of labels that are used:

- Layer 2 point-to-point: Mainly used for high-speed data transmission between sites
- Layer 3 IP VPN: Used in a multi-site environment
- Layer 2 Virtual Private LAN Services: Used for Ethernet services

On a network using MPLS, the data is transported from one node to another using the labels rather than the complex network queries using the routing tables. This reduces the query execution time and speeds up the traffic transmission.

# Multipoint Generic Routing Encapsulation

- Enables one to multi node communication
  - Is used in Dynamic Multipoint VPN deployments
  - Removes the bottleneck of configuring static endpoints by enabling dynamic connections



## What is Multipoint GRE (mGRE) and how does it work? - The Security Buddy

The Multipoint Generic Routing Encapsulation, more commonly known as mGRE is a protocol that creates and terminates connections between nodes on a network. It enables multi-node communication, such as in the point of a VPN. You have one VPN server, and multiple VPN clients connect to the VPN server.

One of the core uses of mGRE is in the Dynamic Multipoint VPN deployments, in which you do not have to pre-configure the endpoints for VPN connectivity. The mGRE protocol uses dynamic connections that create the VPN connections, and in the end, it terminates those connections.

A woman with long brown hair, wearing a white button-down shirt and a black headset with a microphone, is smiling and looking towards the camera. She is seated at a desk with a computer keyboard and a mouse. In the background, another person is visible, and there are plants and office equipment. A purple rectangular overlay contains the text.

**TOPIC 3**

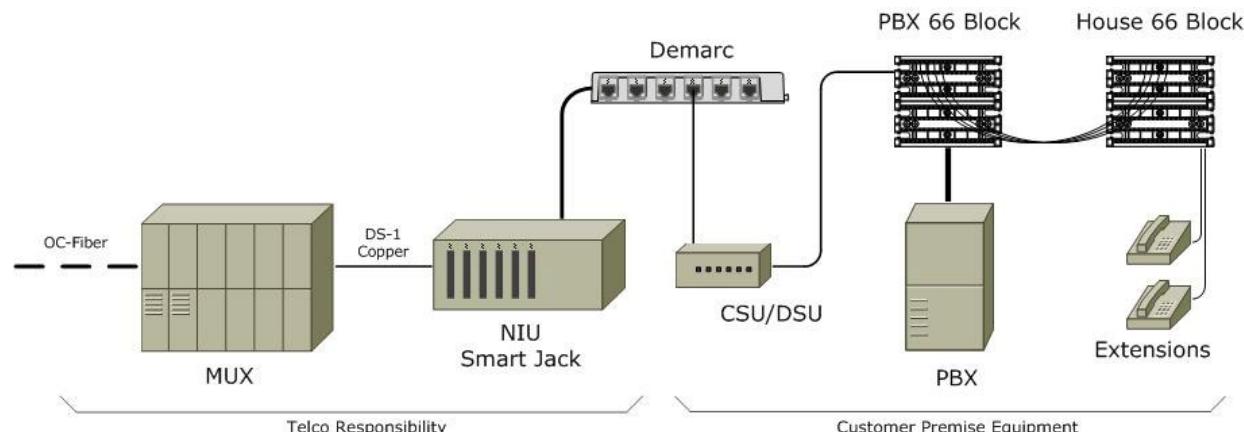
---

# **SERVICE-RELATED ENTRY POINT**

---

# Demarcation Point and Smart Jack

- Demarcation Point
  - Is the hand-off point from one entity to another entity
    - Service provider to the customer
  - Is the point where service provider terminates the connection at customer premises
- Smart Jack
  - Is the equipment for terminating a connection
  - Provides the remote loopback capability to locate errors



## [T1 / DS1 Smart Jack RJ-48C Wiring Explained End to End | Bohack](#)

When your organization takes a leased line or any other connection from a service provider, there has to be a terminating point from the service provider. For example, the service provider will bring the line to a certain point, let's say outside your building, and from there onwards, you need to ensure that you have your arrangements for the connectivity. The point where the service provider terminates the connection is the demarcation point.

Smart jack is the device that is used for terminating the connection. The service providers use the smart jack for remote loopback capability to locate errors in the connection provided to the customer.

## *TOPIC 4*

---

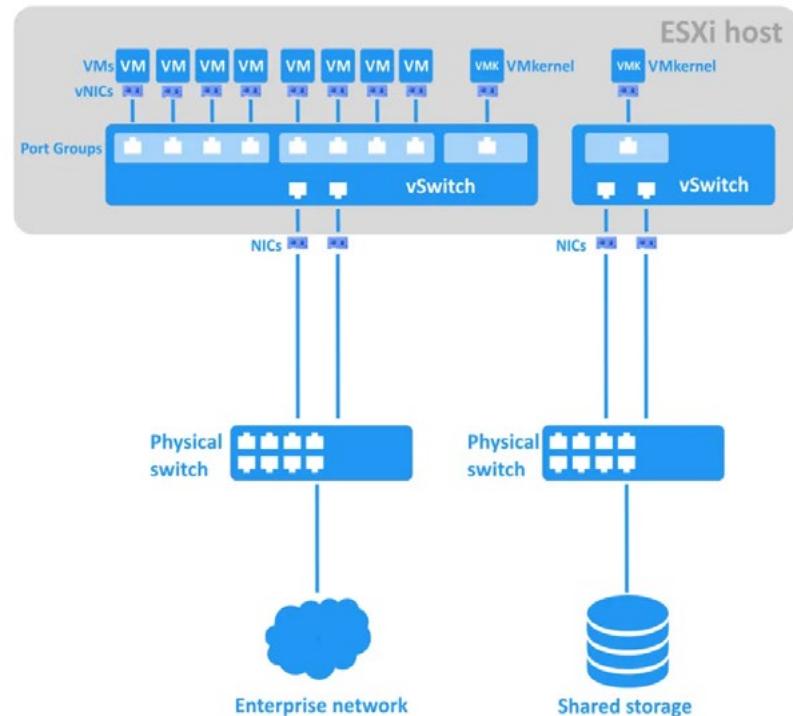
# VIRTUAL NETWORK CONCEPTS

---

# vSwitch

- Works like a physical switch but is a software
- Emulates the layer-2 switch
- Do not work with:
  - MAC address
  - Spanning Tree Protocol
  - Create a network loop for redundancy

[What is a VMware vSwitch? Learn More in This Post  
\(nakivo.com\)](#)



In virtual networking, you have a virtual switch known as vSwitch, a technology offered by VMware. It functions just like a physical switch but is a virtual switch designed to perform the routing functions. When configuring a vSwitch, you do not need any external physical switch to perform routing from your virtual machines. vSwitch works on the hypervisor to perform these functions. If you do not understand the term hypervisor, you do not need to worry, as explained a few slides later.

A vSwitch provides connectivity between the virtual machines and the host if required. It uses the physical network interface card (NIC) to connect with the physical host and the rest of the network. However, you can limit the traffic between the virtual machines only.

vSwitch emulates a Layer 2 switch that replaces a physical switch. It works like a regular physical switch. However, there are fundamental differences between a physical and vSwitch. A physical switch uses the MAC address to forward the traffic to the destination. A vSwitch does not work with the MAC addresses. The other two key differences are that a vSwitch does not use Spanning Tree Protocol (STP) and does not use network loops to create redundant network connections.

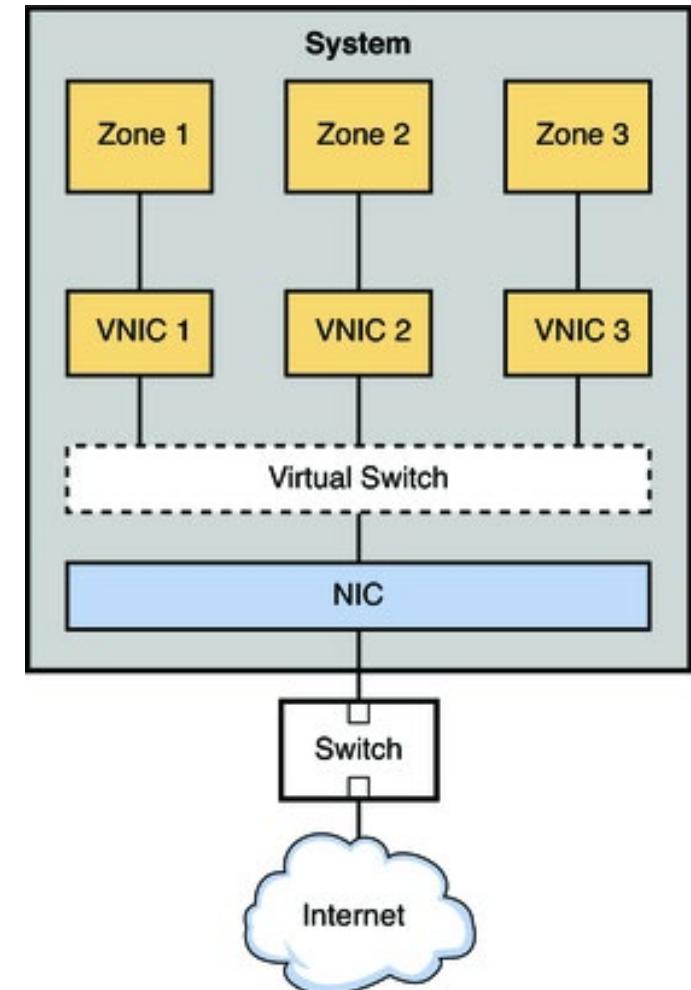
# Virtual Network Interface Card (vNIC)

- Is the virtualized network interface card (vNIC)
- Uses the same sequence as Ethernet adapters:
  - Eth0 as vnic0
  - Eth1 as vnic1
- Is used in virtual machines
- Connects to the virtual switch

## [Network Virtualization and Virtual Networks - Oracle Solaris Administration: Network Interfaces and Network Virtualization](#)

Each device, whether physical or virtual, needs a NIC to communicate. A NIC is a vNIC or virtual network interface card in virtual environments. It is required in each virtual machine to communicate with the hypervisor or even to the host or rest of the physical network. vNIC is the same as the NIC, except it is virtual. You can have several vNIC installed in virtual machines. They are usually numbered as vnic0 or vnic1. The number of the vNIC is incremented by the value of 1.

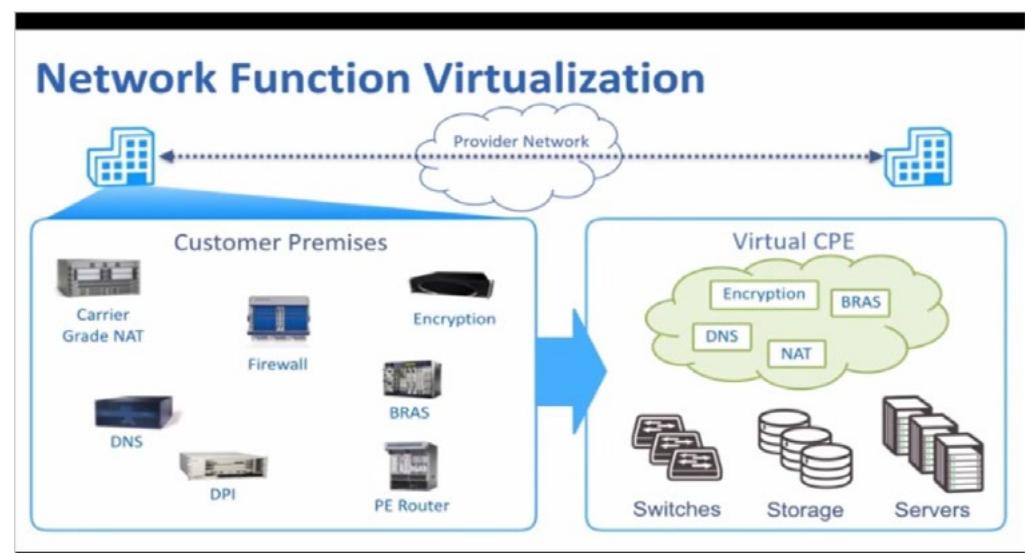
A virtual machine can be configured with one or more vNICs, which in turn connect to the vSwitch.



# Network Function Virtualization (NFV)

- Is a method to virtualize the network services
  - Firewall
  - Router
  - Switches
- De-couples the networking services from the hardware and virtualizes them

[Big opportunities are coming to Pakistan with 5 G and NFV \(Network function Virtualization\) and SDN \(Software Defined Networking\). Job market will expand for all telecom and electronic engineers - CTTC Updates \(typepad.com\)](#)



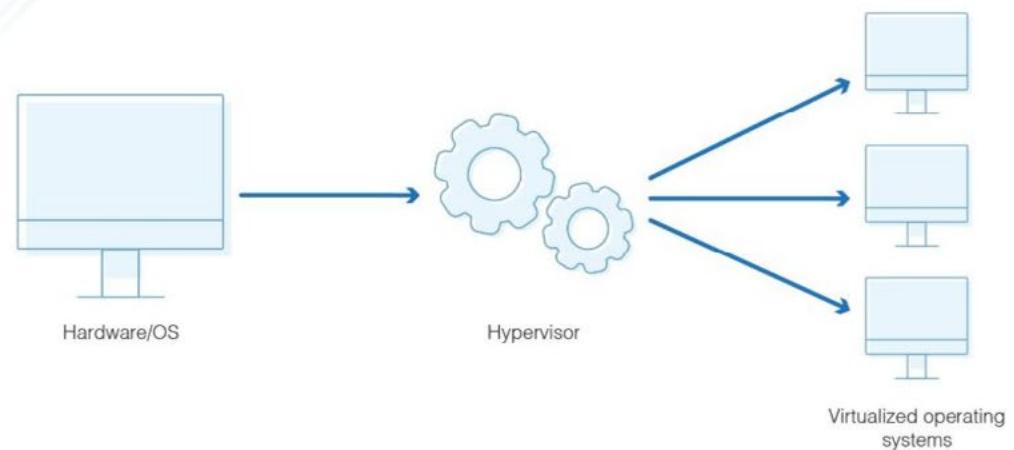
Like a typical physical network, a virtual network also has various networking devices or services like switches, firewalls, and routers. NFV or Network Function Virtualization is a method of virtualizing these services and making them work in the virtual environment. There is no dependency on the hardware appliances or devices because NFV enables them to run in the virtual environment.

# Hypervisor

- Is used to virtualize hardware for virtual machines
- Creates a virtualization layer to separate:
  - RAM
  - CPU
  - Other physical resources
- Are of two types:
- Type 1 Hypervisor - bare metal or native
- Type 2 Hypervisor - hosted hypervisors

[What is a Hypervisor? Types of Hypervisors Explained \(1 & 2\) \(phoenixnap.com\)](https://www.phoenixnap.com/resource/career-development/what-is-a-hypervisor-types-of-hypervisors-explained-1-2)

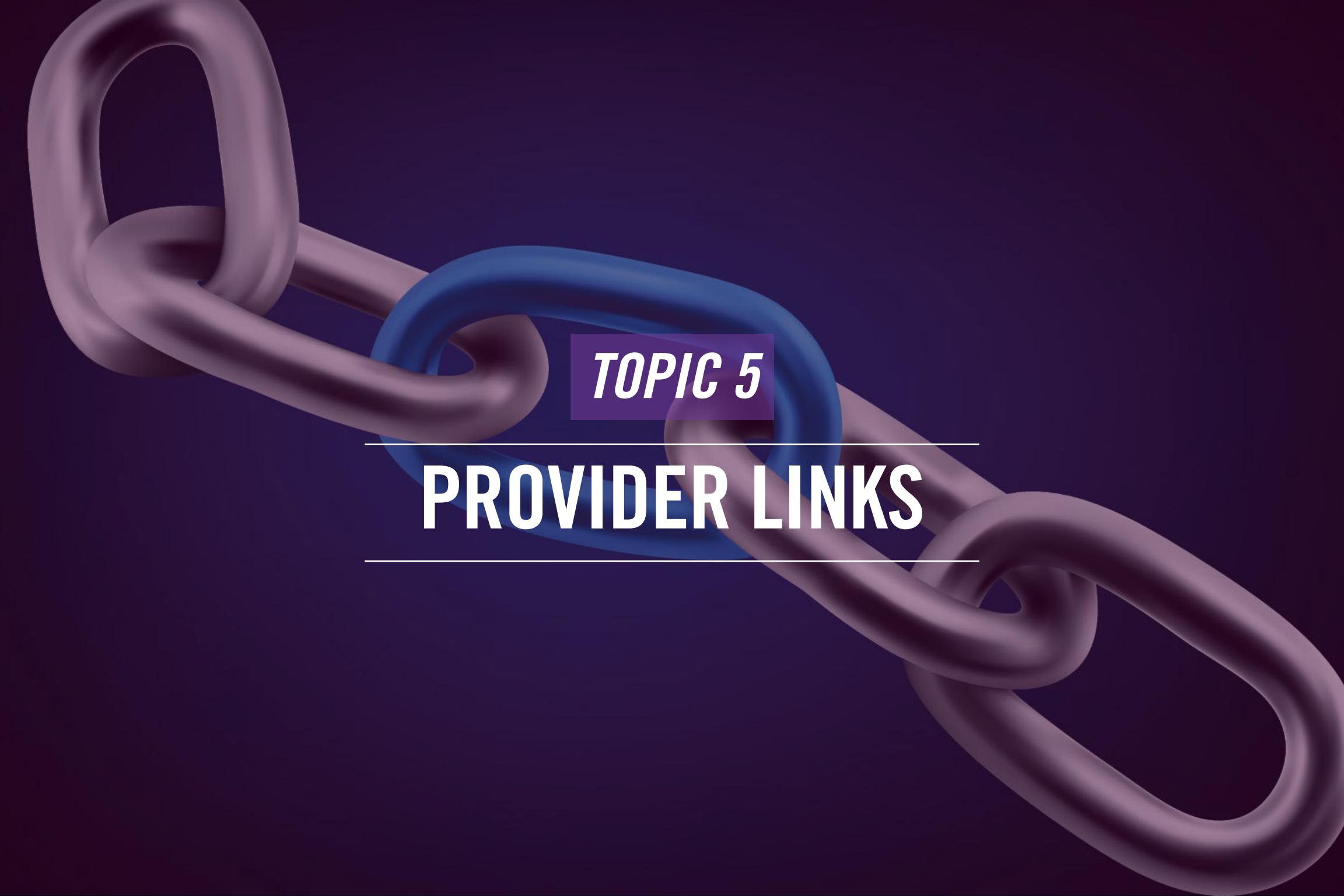
## What Is a Hypervisor?



Each device, whether physical or virtual, needs a NIC to communicate. A NIC is a vNIC or virtual network interface card in virtual environments. It is required in each virtual machine to communicate with the hypervisor or even to the host or rest of the physical network.

vNIC is the same as the NIC, except it is virtual. You can have several vNIC installed in virtual machines. They are usually numbered as vnic0 or vnic1. The number of the vNIC is incremented by the value of 1.

A virtual machine can be configured with one or more vNICs, which in turn connect to the vSwitch.



***TOPIC 5***

---

# PROVIDER LINKS

---

# Service Provider Links

- Satellite
  - Uses satellites to provide Internet connectivity
  - Has a wide reach
- Digital subscriber line (DSL)
  - Uses existing telephone connection for high-speed connectivity
- Cable
  - Uses the traditional cable TV connection to provide Internet connectivity
- Leased line
  - Is exclusive connection for a customer over copper or fiber cables
- Metro-optical
  - Is an optical connectivity that can span over hundreds of kilometers

There can be various connectivity options. Depending on your requirements, you can use one of the service provider links to provide Internet connectivity. Let's look at these options.

Satellite links use satellites to provide Internet connectivity, and they are good if you need a broad reach where the service provider cannot provide any other form of Internet connectivity. For example, a satellite connection is a good option if you are in a mountain area.

Another option is DSL or Digital Subscribers Line. The service provider uses the existing telephone connection to provide high-speed connectivity. For home users, this is an excellent option to use.

Cable Internet connections use the traditional cable TV connection for Internet connectivity. The cable TV service providers usually have extra bandwidth to provide to the customers on a chargeable basis. Leased lines are dedicated connections that are provided to the organizations. They are more reliable because you get a dedicated line for your organization. The connection is provided over copper or fiber optic cables.

Metro-optical is another type of connection that can span over hundreds of kilometers.



# Summary



Mesh



Star/hub-and-spoke



Bus



Ring



Hybrid



Network types and characteristics



Service-related entry point



Virtual network concepts



Provider links



Hi, welcome to COMPTIA Network+ Course In this lesson, we will talk about:

- Mesh
- Star/hub-and-spoke
- Bus
- Ring
- Hybrid
- Network types and characteristics
- Service-related entry point
- Virtual network concepts
- Provider links



*NEXT TOPIC*

---

# CABLES AND CONNECTORS

---

Lesson

3

---

# Cables and Connectors

- 1 — Welcome to the lesson 3 of Module 1. In this lesson, you will learn about the:
  - 2 — Various cables and connectors.
- 



Network Fundamentals

# AGENDA



Copper



Fiber



Connector Types



Cable Management



Ethernet Standards



Hi, welcome to COMPTIA Network+ Course

In this lesson, we will talk about:

- Copper
- Fiber
- Connector Types
- Cable Management
- Ethernet Standards





*TOPIC 1*

---

# COPPER

---

# Copper - Twisted Pair

Ethernet Cable Comparison Chart			
Category	Shielded	Max. Transmission	Max. Bandwidth
Cat 3	No	10 Mbps at 100m	16 MHz
Cat 5	No	10/100 Mbps at 100m	100 MHz
Cat 5e	No	1 Gbps at 100m	100 MHz
Cat 6	Yes & No	1 Gbps at 100m	250 MHz
Cat 6a	Yes	10 Gbps at 100m	500 MHz
Cat 7	Yes	10 Gbps at 100m	600 MHz
Cat 7a	Yes	10 Gbps at 100m	1000 MHz
Cat 8	Yes	25 Gbps/40 Gbps	2000 MHz at 30m

[Ethernet Cable Wiring](#)  
[Ontario - Network Telecom](#)  
[\(network-telecom.com\)](#)

Copper cables are of two types: UTP or Unshielded Twisted-Pair and STP or Shielded Twisted-Pair. The fundamental difference between both the cables is that the STP cable has an extra shield layer inside the outer cover. The extra layer of the shield protects from any interferences.

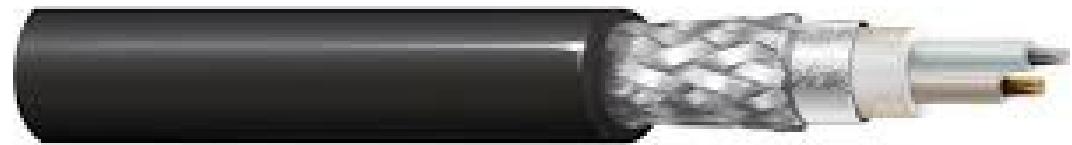
So, there are different types of cables. The CAT 3, 5, and 5e are essentially the UTP cables. CAT 6 is also UTP, but it is also the STP cable. Each one is capable of a specific maximum transmission and bandwidth. Most of them can stretch up to 100 meters except CAT 8, which has a maximum length of 30 meters but provides the highest transmission rate of 25 Gbps.



# Copper – Other Types



[Southwire RG6 Coaxial 150M Coaxial Cable - Black | The Home Depot Canada](#)



[9207 010500 | Belden Twinaxial Cable PVC 8.4mm 100Ohm Tinned Copper Black 152m | Distrelec Germany](#)

The other types of copper cables are RG6 and Twinaxial. The RG6 cable is used in the residential and commercial installation and satellite signals. Its primary usage is for the television signal relay. Because of its prominent conductor, it provides excellent signal quality. The outer side has thick insulation that prevents the signals from any interference.

The twinaxial or commonly known as Twinax, has two conductors. Unlike RG6 that has two conductors, the twinaxial cable has two. It is used where you need short-range and high-speed transmissions.

# Copper - Twisted Pair

TIA/EIA 568A Wiring	
1	Green-White
2	Green
3	Orange-White
4	Blue
5	Blue-White
6	Orange
7	Brown-White
8	Brown

TIA/EIA 568B Wiring	
1	Orange-White
2	Orange
3	Green-White
4	Blue
5	Blue-White
6	Green
7	Brown-White
8	Brown

© OmniSecu.com

The termination order determines the order used for placing the wires within an RJ45 connector. The termination can be done based on the Telecommunications Industry Association (TIA)/Electronic Industries Alliance (EIA) standards for Unshielded Twisted Pair wiring, TIA/EIA 568A & TIA/EIA 568B.

Both TIA/EIA 568A and TIA/EIA-568B standards are pretty much the same. The only difference is that the green and orange wires switch places. The termination of wires also determines whether it will be a straight or crossover cable.

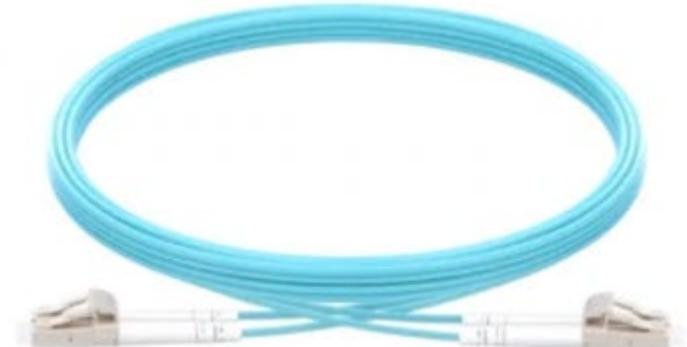
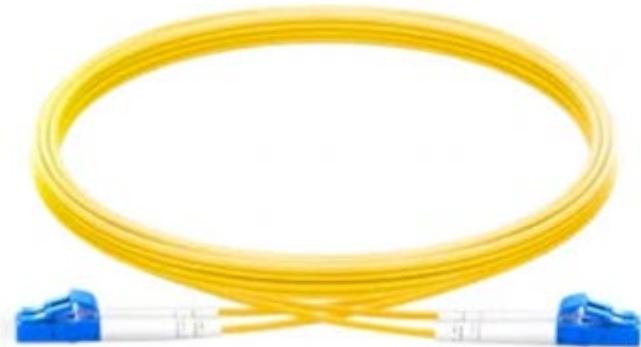
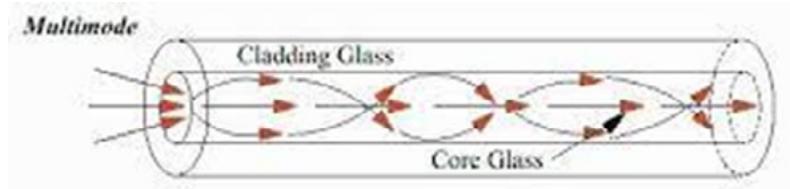
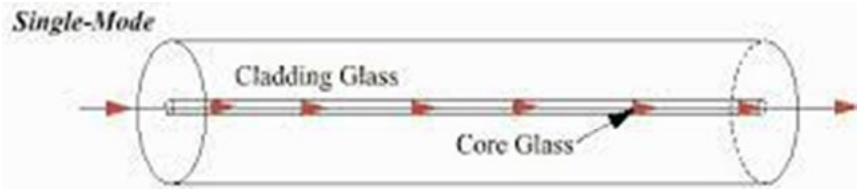
For example, if you have TIA/EIA 568A on both ends of the cable, then you have a straight cable. The same goes for the TIA/EIA 568B on both ends. However, if you terminate TIA/EIA 568A on one end and TIA/EIA 568B on the other end, then you get a crossover cable.



## TOPIC 2

# FIBER

# Single-Mode and Multimode



Fiber cables can either be single mode or multimode. Let's understand the differences between both of them.

The simplest way to understand the differences is that a single-mode fiber generates a single light mode. The multimode fiber generates several light modes simultaneously. A single optical core is 9 $\mu\text{m}$  but 50 $\mu\text{m}$  in the optical core. However, another variant of multimode with 62.5 $\mu\text{m}$  core also exists.

Because there is a single optical core, the data can be transmitted longer distances than the multimode fiber cable.

Let's move to the next slide to see some technical differences between the two.

# Single-Mode and Multimode

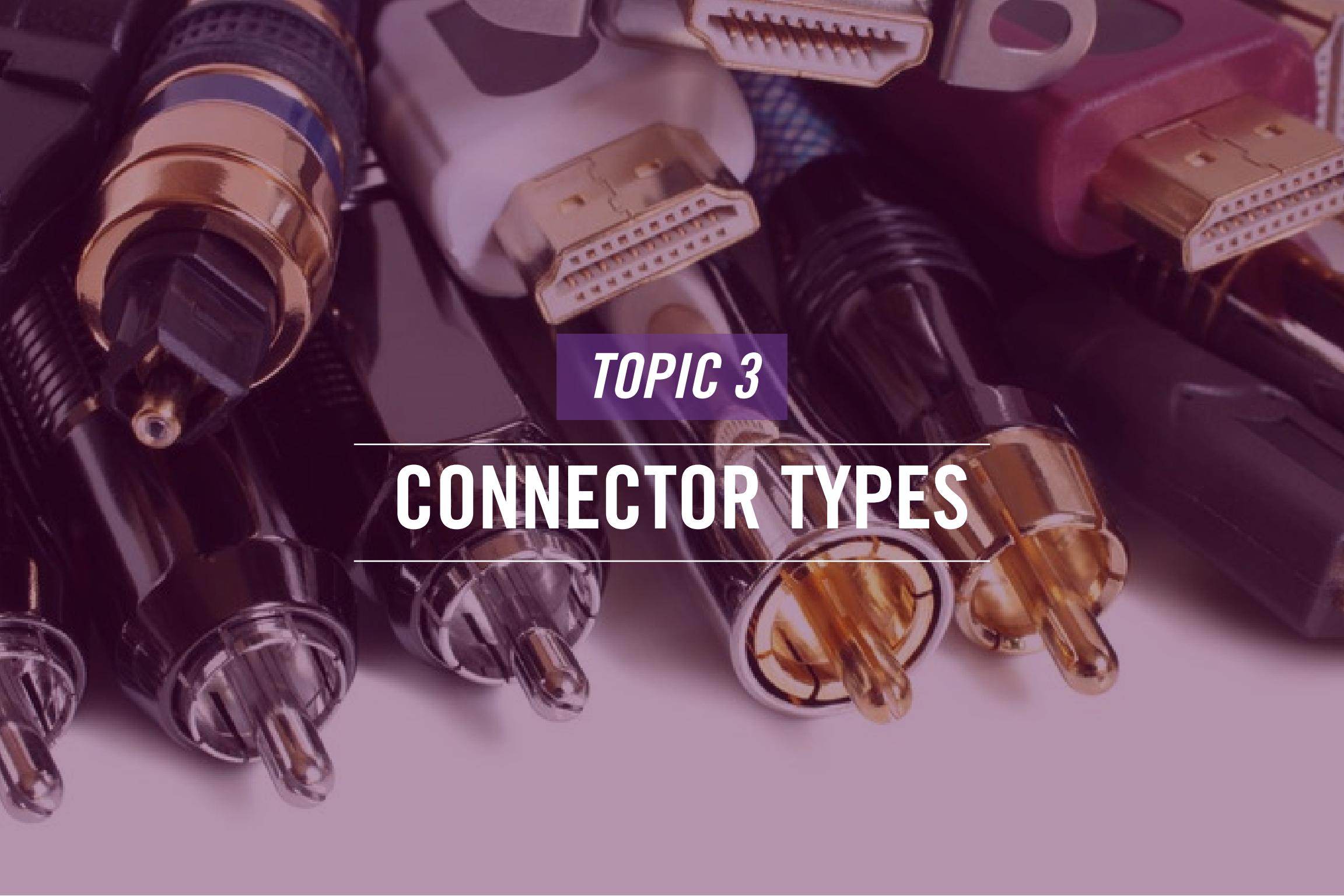
Typical Signal Transmission Distances by Fiber Grade/Type						
Grade	Type	Typical Core Size	1 Gb Distance	10 Gb Distance	40 Gb Distance	100 Gb Distance
<b>OM1</b>	Multimode	62.5µm	300m / 1,000 ft.	36m / 118 ft.	Not Recommended	Not Recommended
<b>OM2</b>	Multimode	50µm	550m / 1,800 ft.	86m / 282 ft.	Not Recommended	Not Recommended
<b>OM3</b>	Multimode	50µm	1,000m / 3,280 ft.	300m / 1,000 ft.	100m / 330 ft.	100m / 330 ft.
<b>OM4</b>	Multimode	50µm	1,000m / 3,280 ft.	550m / 1,800 ft.	125m / 410 ft.	125m / 410 ft.
<b>OS1</b>	Single mode	9µm	2,000m / 6,560 ft.	2,000m / 6,560 ft.	Not Recommended	Not Recommended
<b>OS2</b>	Single mode	9µm	10km / 6.2 miles	10km / 6.2 miles	10km / 6.2 miles	10km / 6.2 miles
<b>Resolution</b>				<b>1080p</b>	<b>4K HDR</b>	<b>8K</b>

## [Single Mode vs. Multimode Fiber... What's the Difference? | TechLogix Networkx \(tlnetworkx.com\)](#)

This slide lists some of the differences between single-mode and multimode. As stated in the previous slide, the data can be transmitted longer distances than the multimode fiber cable on a single optical core. For example, multimode goes up to 1000 meters or 3280 feet, but a single mode can go up to 10 kilometers or 6.2 miles. The distance of specific data size includes 4K HDR and 8 K video, for example. The slide also mentions the cables, whether single-mode or multimode, that are whether recommended or not for specific video resolutions.

A single mode has more light sources that have lower attenuation. On the other hand, multimode fiber has several light modes with higher attenuation.





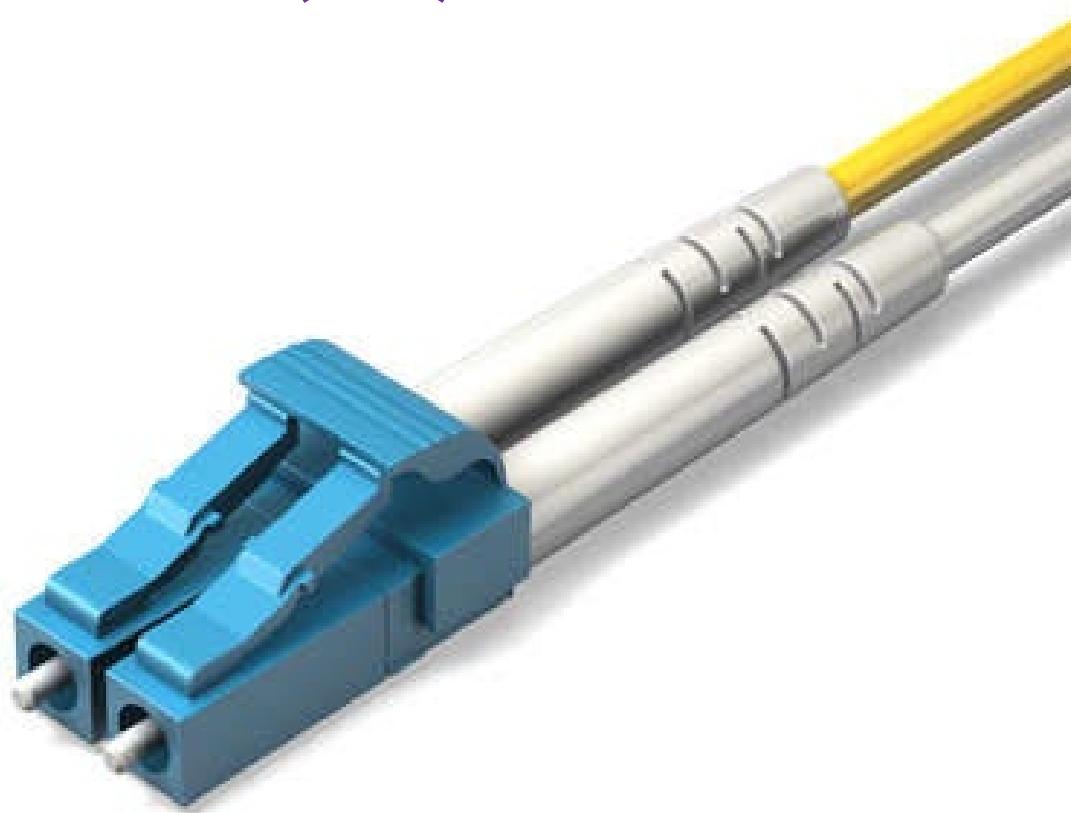
*TOPIC 3*

---

# CONNECTOR TYPES

---

# Local connector (LC)



[Types of Fiber Optic Cables and Connectors \(meridianoutpost.com\)](http://meridianoutpost.com)

LC acronym denotes Lucent Technology. It is a small form-factor connector standardized as Fiber Optic Connector Intermateability Standards (FOCIS 10) in EIA/TIA-604-10. LC connector is available as LC Duplex and LC Simplex connector. It has an easily adjustable design. It can be easily plugged into the slot and taken out with its clip. In short, it does not require any installation.

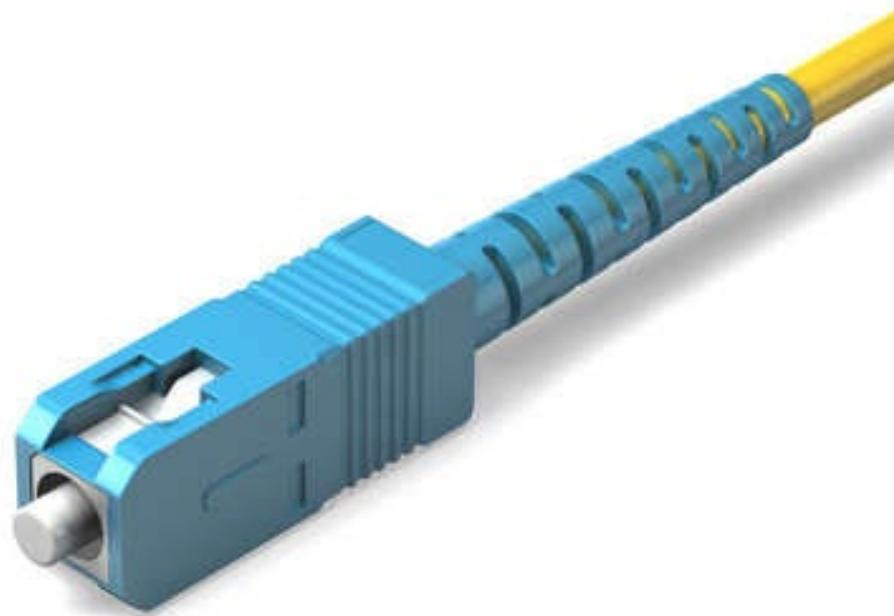
# Straight Tip (ST)



[Types of Fiber Optic Cables and Connectors \(meridianoutpost.com\)](http://meridianoutpost.com)

The ST connector has a half-twist bayonet lock that has been standardized as Fiber Optic Connector Intermateability Standards (FOCIS 2) in EIA/TIA-604-02. The ST connector has a bayonet mount and 2.5 mm ceramic ferrule that holds the fiber.

# Subscriber Connector (SC)



[Types of Fiber Optic Cables and Connectors \(meridianoutpost.com\)](http://meridianoutpost.com)

SC is a FOCIS-3 (TIA-604-3) compliant fiber connector with a 2.5 mm ferrule. It is a snap-in connector that fits into the socket. You can use the latch given above on the connector to release the connector from the socket.

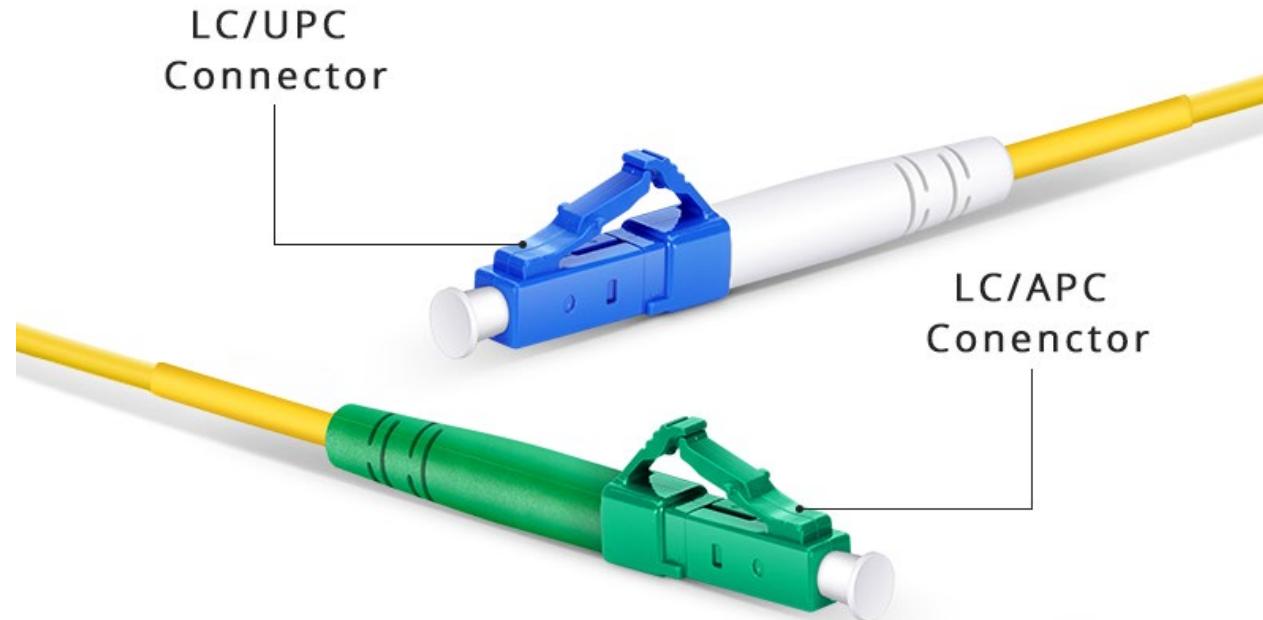
# Mechanical Transfer (MT)



[Types of Fiber Optic Cables and Connectors \(meridianoutpost.com\)](http://meridianoutpost.com)

MJ-RJ or Mechanical Transfer Registered Jack is a fiber connector standardized as FOCIS 12 in EIA/TIA-604-12. Its shape is similar to the shape of an RJ-45 connector. One of the critical advantages of the MT-RJ connector was that it had a small form factor as compared to the SC and ST connectors. It also benefited from having TX and RX strands in a single connector.

# Registered Jack (RJ)

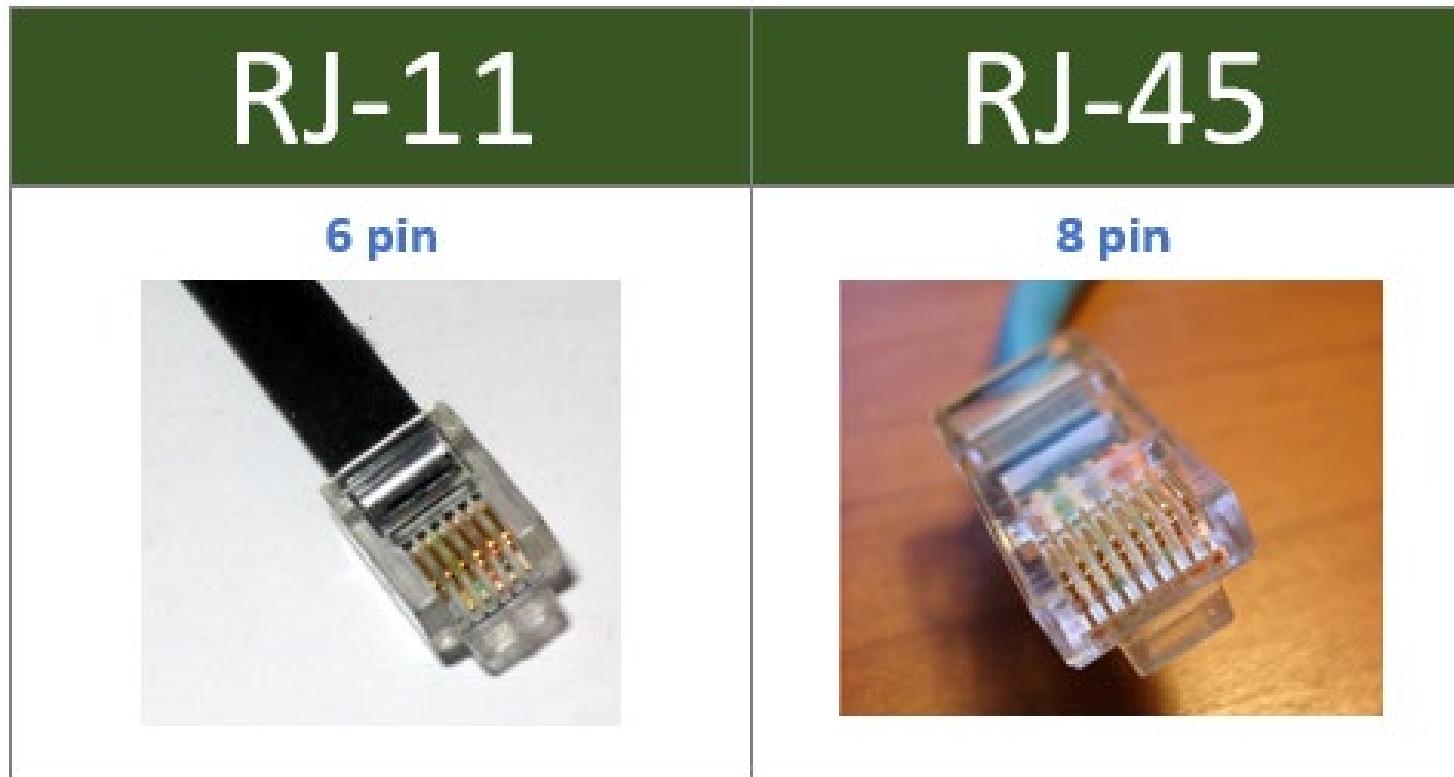


## PC vs UPC vs APC Connector: Selecting the Right Fiber Connector Type | FS Community

There are two types of registered jacks. The first one is UPC, Ultra Physical Contact. The second one is APC, Angled Physical Connect. Let's look at the UPC connector first. UPC is an improved version of the PC connector generally used with the OM1 and OM2 multimode fiber. The UPC connectors are generally blue. The UPC connectors are generally used in digital TV and telephony.

APC has a polished ferrule endface with a radius of an 8° angle to minimize the back reflection. APC should be used where you need high-precision fiber signals. If you have applications that cannot work with heavy return loss, you should use the APC connectors. The APC connector should only be used with the other APC connectors for better signals. The APC connectors are generally green in color.

# RJ<sub>11</sub> / RJ<sub>45</sub>



[RJ45 vs RJ11: What is the difference between RJ45 and RJ11? \(router-switch.com\)](http://router-switch.com)

RJ11 and RJ45 look the same but except for their sizes. The RJ45 connector is almost double and used with the Ethernet cables. RJ11 is used with the telephone cables. The RJ11 connector has 6-pins, whereas the RJ45 connector has 8-pins with 8 wires. RJ11 connector has only four wires.

# F-type Connector



[Professional Series RG6 F-Type Coax Cable | ShowMeCables.com](https://www.showmecables.com/professional-series-rg6-f-type-coax-cable)

An F-type connector is a round-shaped connector that two-wires, one of which is signal and ground cable. The F-type connector is used with the set-top boxes, cable modems, and hybrid fiber coax networks.

# Transceivers/Media Converters

[What is Media Converters | Function of Media Converters in Network | Data flow through the Media Converters in a network \(generalnote.com\)](#)



A transceiver is built into the network interface cards but can also be a separate hardware device. A device with transceiver capabilities can transmit and receive signals, whether an independent device or a network interface card.

A media converter is a hardware device that connects two different media types, such as fiber and twisted pair. You may need to connect a fiber network with an Ethernet or Gigabit Ethernet. In such a case, you will need to have a media converter to connect both the ends of the networks to communicate between them.

# Transceiver Type

Small form-factor pluggable (SFP)



[Small Form Factor Pluggable Transceiver, ॲप्टिकल ट्रान्ससीवर -  
Balaji Enterprises, Ghaziabad | ID: 18259508091 \(indiamart.com\)](#)

Enhanced form-factor pluggable (SFP+)



[DEM-432XT - 10GBase-LR SFP+ Transceiver \(Singlemode  
1310nm\) - 10km - D-Link Philippines \(dlink.com.ph\)](#)

There are different types of transceivers. Let's look at the four primary types. First, you have a small form-factor pluggable (SFP) transceiver, which is compact and hot-swappable. It is mainly used in data communication and telecommunications networks. Its primary purpose is to convert optical and electrical signals.

SFP+ is an improved and enhanced version of the SFP that can support different types of network media, such as 8 Gbit/s Fibre Channel and 10 Gigabit Ethernet. Similar to SFP, the Quad Small Form-factor Pluggable (QSFP) is also compact and hot-pluggable. It is mainly used for data communications. It allows the data rate of 4×1 Gb/s. It can connect with the servers and switches by terminating the fiber optic connection.

QSFP+ is an extended form of QSFP that can support a data rate of 4×10 Gbit/s.

# Transceiver Type

Quad small form-factor pluggable (QSFP)



[Quad Small Form-factor Pluggable | Xiangyi Xu |](#)

[Washington University in St. Louis \(wustl.edu\)](#)

Enhanced quad small form-factor pluggable (QSFP+)



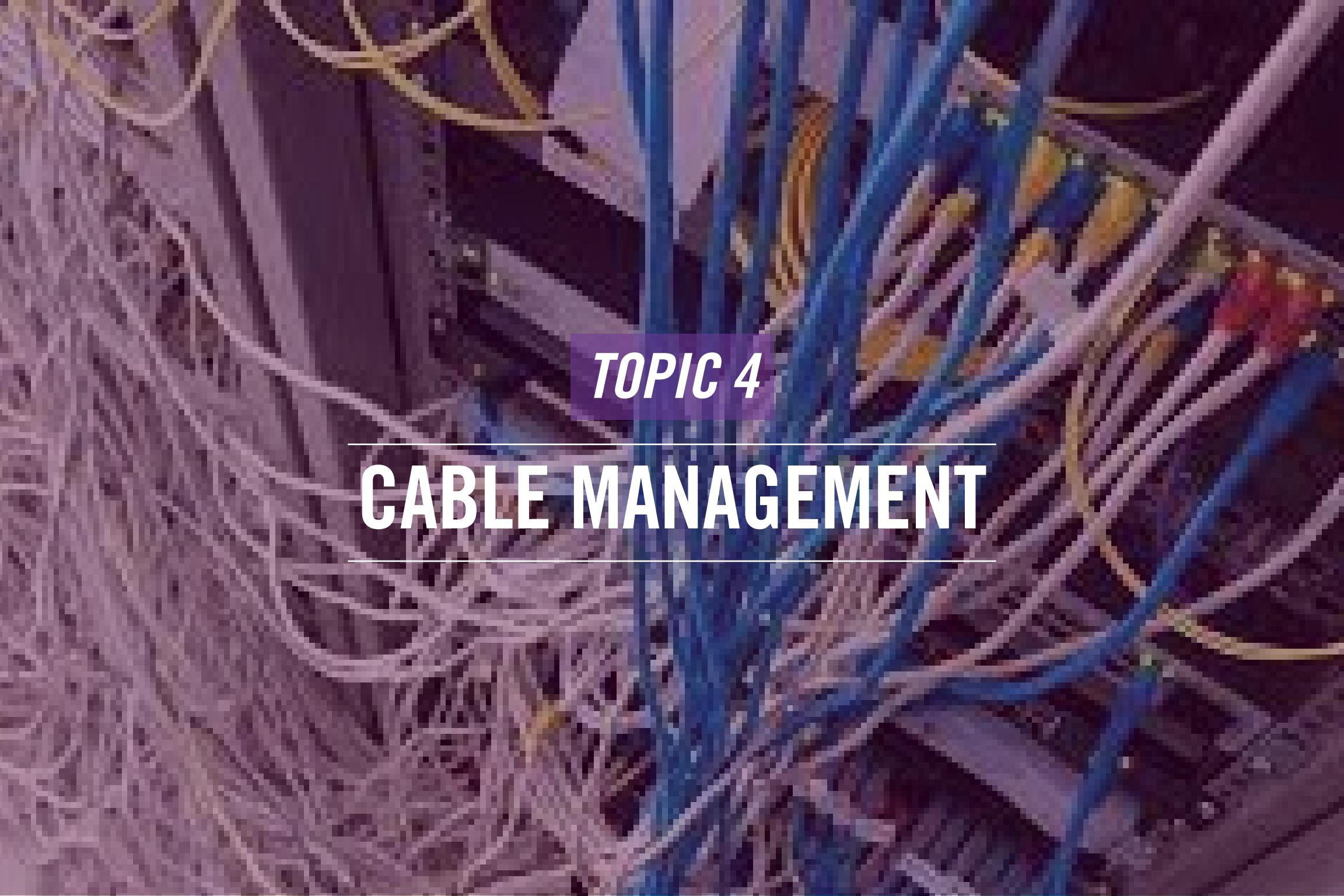
[40gbase-Lr4 SMF QSFP + Optical Transceiver](#)

[1310nm 10km For Data Centers](#)

There are different types of transceivers. Let's look at the four primary types. First, you have a small form-factor pluggable (SFP) transceiver, which is compact and hot-swappable. It is mainly used in data communication and telecommunications networks. Its primary purpose is to convert optical and electrical signals.

SFP+ is an improved and enhanced version of the SFP that can support different types of network media, such as 8 Gbit/s Fibre Channel and 10 Gigabit Ethernet. Similar to SFP, the Quad Small Form-factor Pluggable (QSFP) is also compact and hot-pluggable. It is mainly used for data communications. It allows the data rate of  $4 \times 1$  Gb/s. It can connect with the servers and switches by terminating the fiber optic connection.

QSFP+ is an extended form of QSFP that can support a data rate of  $4 \times 10$  Gbit/s.



*TOPIC 4*

---

# CABLE MANAGEMENT

---

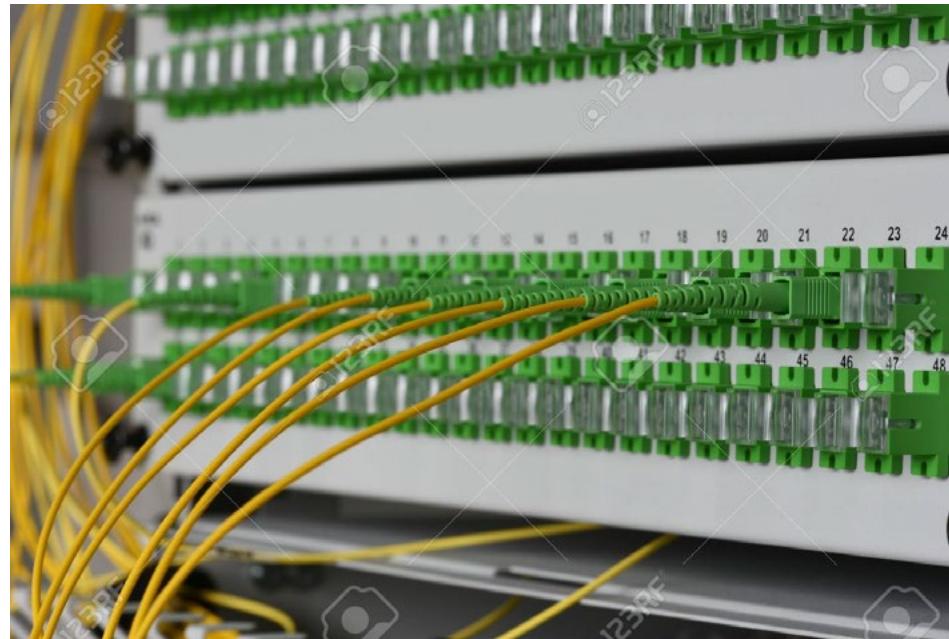
# Patch Panel/Patch Bay



[Patch panel, 24a-port, STP, cat. 6, 1U, 19", IDC 110, with LED \(atel-electronics.eu\)](http://atel-electronics.eu)

You must have seen the wall outlets for Ethernet connections where you plug in the cable to connect to the network. The wall outlet for Ethernet connects to the patch panel, which is housed in a rack in a data center. The patch panels have the wall outlets' connections terminated in the back and from the front sockets, they connect to a switch. The patch panels help you organize the cables cleanly and systematically.

# Fiber Distribution Panel



[Distribution Panel Of Fiber Network With Optical Network Cables Stock Photo, Picture And Royalty Free Image. Image 96373151. \(123rf.com\)](#)

There are different types of transceivers. Let's look at the four primary types. First, you have a small form-factor pluggable (SFP) transceiver, which is compact and hot-swappable. It is mainly used in data communication and telecommunications networks. Its primary purpose is to convert optical and electrical signals.

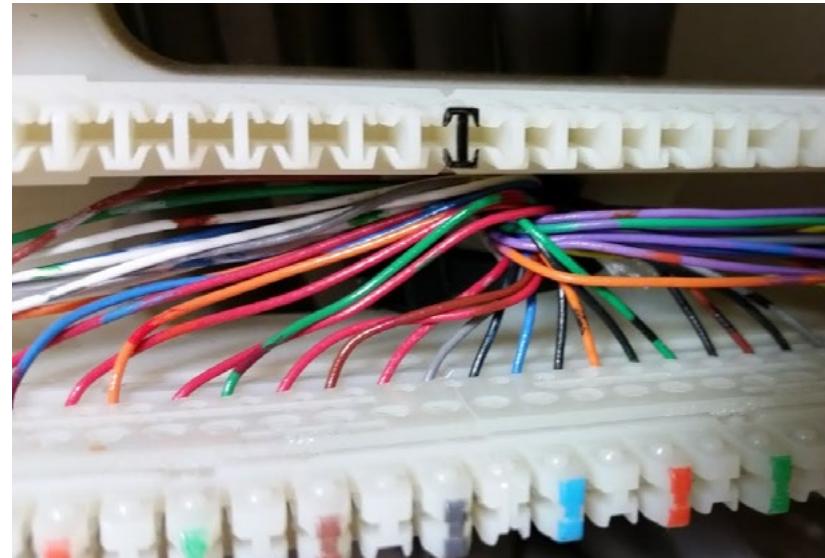
SFP+ is an improved and enhanced version of the SFP that can support different types of network media, such as 8 Gbit/s Fibre Channel and 10 Gigabit Ethernet. Similar to SFP, the Quad Small Form-factor Pluggable (QSFP) is also compact and hot-pluggable. It is mainly used for data communications. It allows the data rate of  $4 \times 1$  Gb/s. It can connect with the servers and switches by terminating the fiber optic connection.

QSFP+ is an extended form of QSFP that can support a data rate of  $4 \times 10$  Gbit/s.

# Punchdown Blocks



[Network Fun!!! -- A Security/Network Engineer's Blog:](#)  
[66 Block Punch Downs \(shanekillen.com\)](#)



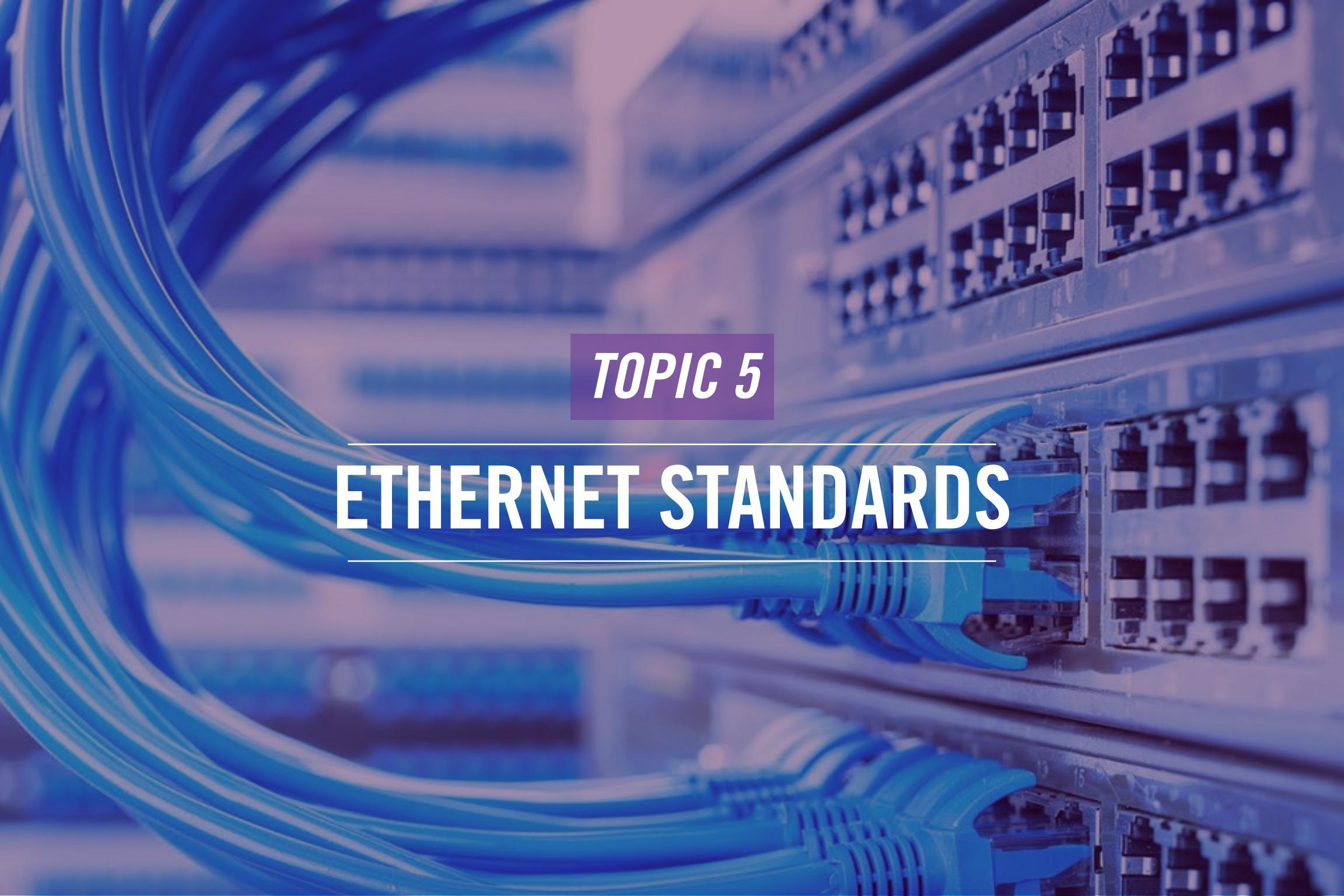
[punch down 110 blocks - YouTube](#)

A punchdown block is used for punching the cables into a slot. You can punch a cable into the slot using a punchdown tool. The cable is placed on the punchdown block and pushed into the slots using a punchdown tool.

There are different variants of the punchdown block. The first one is the 66 block used with the analog telephone systems. The second type of 110 blocks is used for the telephone and CAT 5 cables. It has replaced the older and obsolete version, which is 66 blocks.

The third is the Krone block, a European version of the 110 blocks. It is used for audio interconnections.

The fourth one is the BIX block, proprietary development of the Nortel Networks. It is mainly designed for the CAT 5e cables.



*TOPIC 5*

---

# ETHERNET STANDARDS

---

# Ethernet Standards - Copper

Cable	Speed	Range
10BASE-T	10 Mbps	100 m
100BASE-TX	100 Mbps	100 m
1000BASE-T	1 Gbps	100 m
10GBASE-T	10 Gbps	55 m (Cat6), 100 m (Cat6a)
40GBASE-T	40 Gbps	30 m

This slide displays the different Ethernet standards for copper cables. The cable name has a number as a prefix, determining the speed. For example, in 10Base-T, the number 10 denotes 10 Mbps speed. Similarly, in 40GBASE-T, it is 40 Gbps. The table displays three tables. The first column displays the name of the cable. The second column displays the speed, and the third column displays the transmission range that is supported by the cable.



# Fiber Distribution Panel

Cable	Speed	Range
100BASE-FX	10 Mbps	412 m (half-duplex), 2 km (full-duplex)
100BASE-SX	100 Mbps	300 m
1000BASE-SX	1 Gbps	550 m
1000BASE-LX	1 Gbps	500 m (MMF), 5 km (SMF)
10GBASE-SR	10 Gbps	33 m - 400 m
10GBASE-LR	10 Gbps	10 km
Coarse wavelength division multiplexing (CWDM)	10 Gbps	70 km
Dense wavelength division multiplexing (DWDM)	400 Gbps per channel	1000 m
Bidirectional wavelength division multiplexing (WDM)	10 Gb/s, 40 Gb/s, 100 Gb/s, 200 Gb/s, 400 Gb/s and 800 Gb/s	>1000 km

This slide displays the different Ethernet standards for fiber cables. The cable name has a number as a prefix, determining the speed. For example, in 100Base-FX, the number 100 denotes 100 Mbps speed. The second column displays the speed, and the third column displays the transmission range that is supported by the cable.



# Summary



Copper



Fiber



Connector Types



Cable Management



Ethernet Standards



That's the end of the lesson.

Here we covered:

- Copper
- Fiber
- Connector Types
- Cable Management
- Ethernet Standards

**NEXT TOPIC**

---

# IP ADDRESSING SCHEMES

---

Lesson

# 4

# IP Addressing Schemes

- 1 — Welcome to the lesson 4 of Module 1. In this lesson, you will learn about the:
- 2 — IP addressing schemes. So, let's get going.



Network Fundamentals

# AGENDA



Public vs. private



IPv4 vs. IPv6



IPv4 Subnetting



IPv6 Concepts



Virtual IP (VIP)

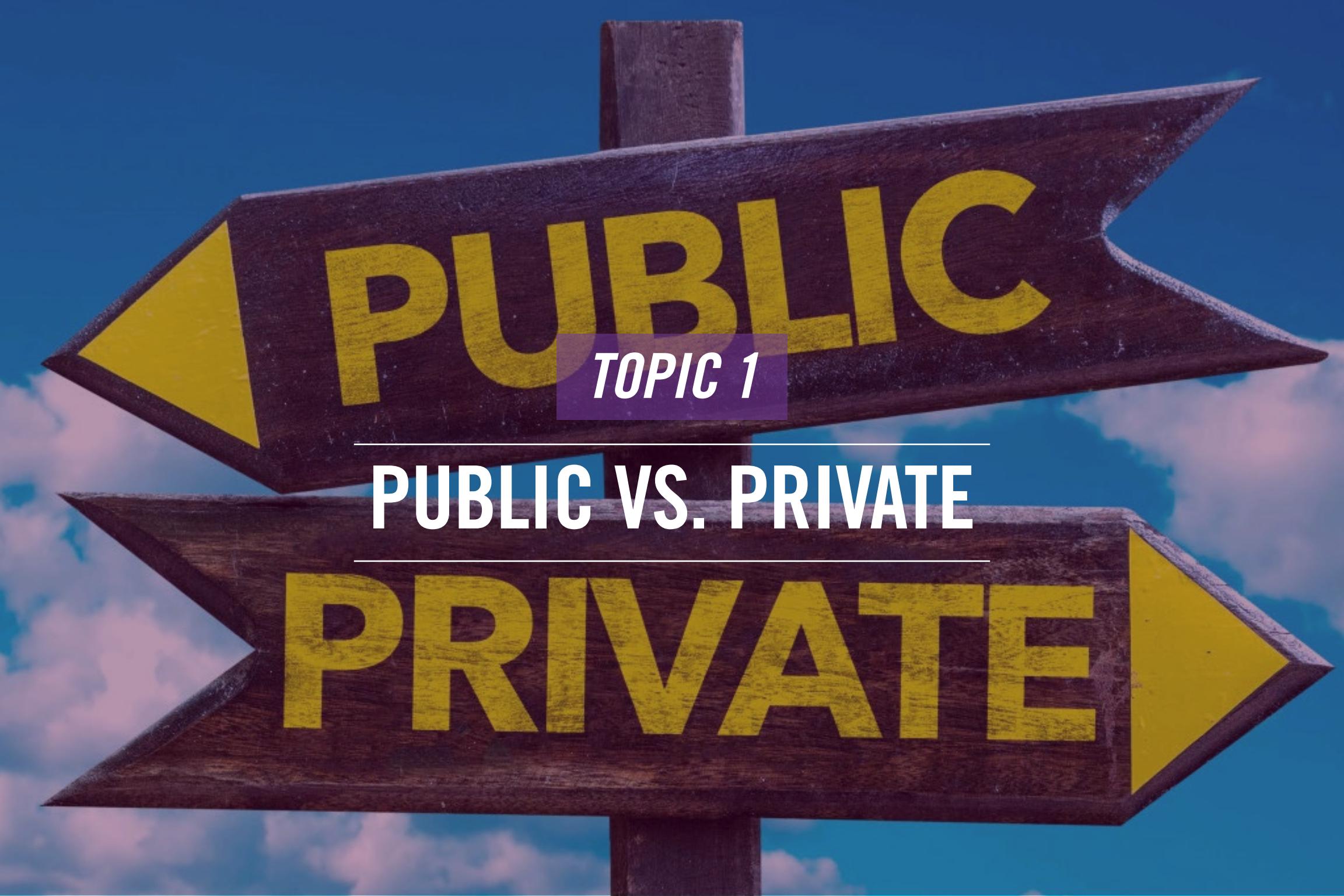


Hi, welcome to COMPTIA Network+ Course

In this, we will talk about:

- Public vs. private
- IPv4 vs. IPv6
- IPv4 Subnetting
- Public vs. private
- IPv4 vs. IPv6
- IPv4 Subnetting





**PUBLIC**

*TOPIC 1*

---

**PUBLIC VS. PRIVATE**

---

**PRIVATE**

# RFC 1918

Port address  
translation (PAT)

Network address  
translation (NAT)

RFC1918

- Are the IP addresses that are assigned to the internal systems in an organization
- Cannot be used on the Internet
- Has three categories:
  - 10.0.0.0 – 10.255.255.255
  - 172.16.0.0 – 172.31.255.255
  - 192.168.0.0 – 192.168.255.255

IP addresses that can be assigned to network devices and systems are of two types: private and public. An organization uses the private IP addresses for the internal systems and public IP addresses for the exposed systems on the Internet. RFC 1918 defines the private IP addresses that can be used only internally in an organization. They cannot be used on the Internet.

A system on the Internet must have a unique public IP address. Several organizations use private IP addresses. For example, organizationA can use the 192.168.10.0 series, and organizationB can use the same. Therefore, the RFC 1918 IP addresses are reserved only for the internal systems.

IP addresses are divided into three categories, known as classes:

- Class A: 10.0.0.0 – 10.255.255.255
- Class B: 172.16.0.0 – 172.31.255.255
- Class C: 192.168.0.0 – 192.168.255.255



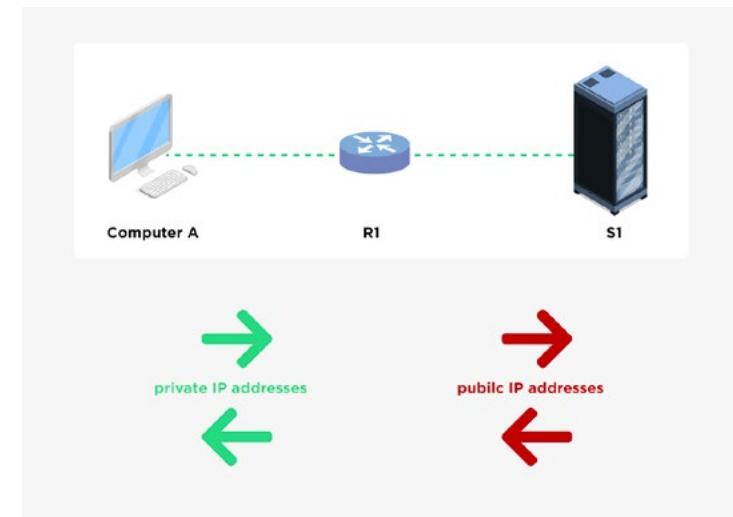
# Network Address Translation (NAT)

Port address translation (PAT)

Network address translation (NAT)

RFC1918

- Allows the internal hosts to communicate on the Internet
- Enables several internal IP addresses to use a single public IP address
- Can be configured on a firewall, a router, or a dedicated device



IP addresses that can be assigned to network devices and systems are of two types: private and public. An organization uses the private IP addresses for the internal systems and public IP addresses for the exposed systems on the Internet. RFC 1918 defines the private IP addresses that can be used only internally in an organization. They cannot be used on the Internet.

A system on the Internet must have a unique public IP address. Several organizations use private IP addresses. For example, organizationA can use the 192.168.10.0 series, and organizationB can use the same. Therefore, the RFC 1918 IP addresses are reserved only for the internal systems.

IP addresses are divided into three categories, known as classes:

- Class A: 10.0.0.0 – 10.255.255.255
- Class B: 172.16.0.0 – 172.31.255.255
- Class C: 192.168.0.0 – 192.168.255.255

[What is NAT \(manageengine.com\)](http://What is NAT (manageengine.com))

# Port Address Translation (PAT)

Port address  
translation (PAT)

Network address  
translation (NAT)

RFC1918

- Is a type of NAT configuration
- Is also known as overloading that uses dynamic NAT
- Uses IPv4 addresses along with the port numbers
- Maps private IP addresses to a single public IP address
  - Uses different ports
  - Performs many-to-one configuration

PAT or Port Address Translation is a type of NAT. It is also known as overloading that uses dynamic NAT. PAT works pretty much in the same manner as NAT. It allows several private IP addresses to communicate over the Internet using a single public IP address. The difference PAT brings in is that it uses different port numbers along with the internal IP addresses. However, this is a typical NAT functionality.

For example, let's consider a scenario of an FTP server, a Web server, and a Web application server. Each one of them uses a different port. You have configured the FTP server with port 21, Web server with port 80 and 443, and Web application server with port 8080.

When the traffic is returned from the Internet after a request is made by, let's say, the FTP server, the traffic is coming to a specific port. The NAT device or server reads the port information and forwards the traffic to the required server.

In PAT, you are using different ports in a many-to-one configuration.





*TOPIC 2*

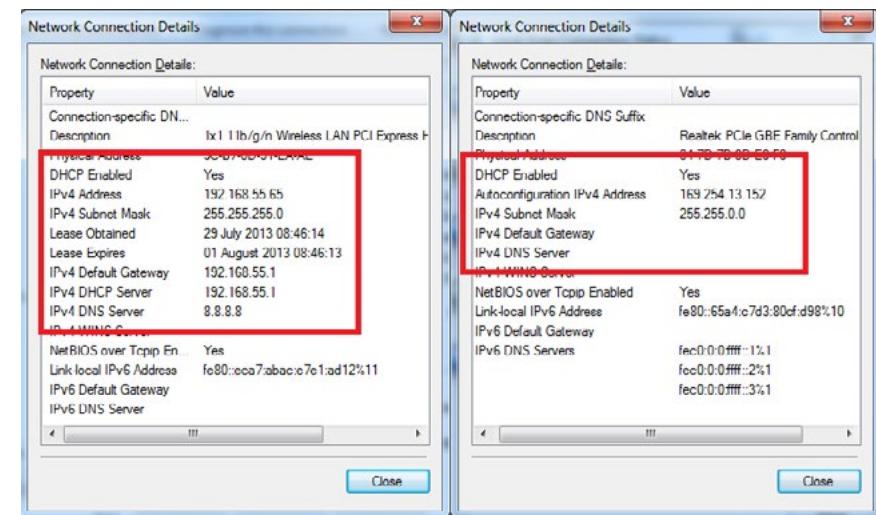
---

# IPV4 VS. IPV6

---

# Automatic Private IP Addressing (APIPA)

- Is an IP address that is assigned to a system when the DHCP server is not available
- Uses the following:
  - Range: 169.254.0.1 through 169.254.255.254
  - Subnet Mask: Class B – 255.255.0.0
- Is not a routable IP address



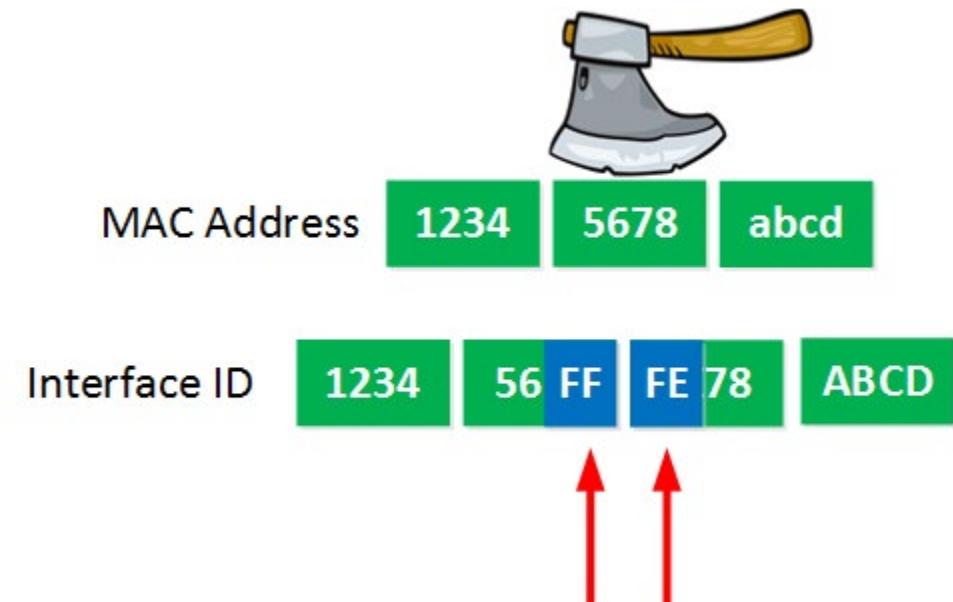
[169.254.what.is.it.suitable.for?/bluecompute.co.uk](http://169.254.what.is.it.suitable.for?/bluecompute.co.uk)

Automatic Private IP Addressing or APIPA is an IP address assigned to a system when it does not receive an IP address from a DHCP server. Let's assume that the DHCP server is down and cannot lease IP addresses to the networked clients. In this scenario, the systems will use the APIPA IP addresses. They will start getting IP addresses from 169.254.0.1 to 169.254.255.254 with a subnet mask of 255.255.0.0. The networked clients will get their IP addresses as the DHCP server becomes available. The APIPA IP addresses will be removed from the systems.

APIPA IP addresses are not routable.

# Extended unique identifier (EUI-64)

- Allows a host to assign an IPv6 address
- Is obtained through a 48-bit MAC address
- Completes 64-bit address with the insertion of 16-bit 0xFFFF
  - The 48-bit is split into 2x24-bits
  - 16-bit 0xFFFF is inserted in the middle of both 24-bits



The host uses its MAC address to generate the IPv6 address. The IPv6 address is 64-bit that is generated using the 48-bit MAC address. However, the problem is that there is a difference of 16-bits because the IPv6 address needs to be 64-bits, and you have only 48-bits from the MAC address. An extra 16-bit 0xFFFF is added to the MAC address to resolve this.

The MAC address is split into two parts of 24-bits. The missing gap of 16-bits is added using FF and EE in the middle of both the 24-bits, which finally completes the 64-bit IPv6 address.

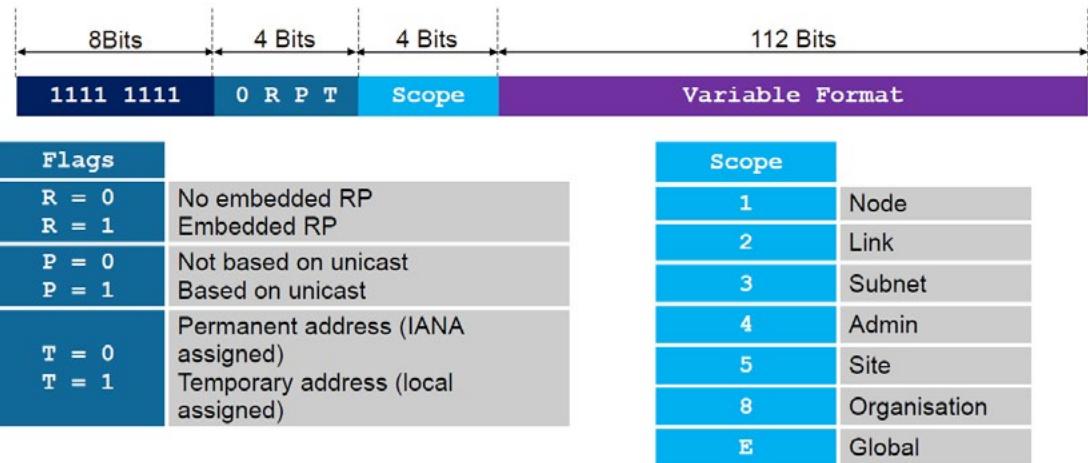
# Multicast

- Identifies multiple interfaces
- Is used for one-to-many communication
- Is always used as the destination address
- Starts with FF
- Uses Format Prefix 1111 1111

## IPv6 Multicast Address (RFC 4291)

An IPv6 multicast address has the prefix FF00::/8 (1111 1111)

- Second octet defines lifetime and scope



[IPv6 Basics | mrn-cciew \(mrncciew.com\)](http://mrn-cciew.com)

A multicast address is used to identify multiple interfaces used for one-to-many communication. When multicast addresses are used, packets are sent to all the interfaces using the multicast addresses. A multicast address is never a source address, but always an address that defines a destination. Format Prefix 1111 1111 is used to identify a multicast address. A multicast address always begins with FF.

A multicast address has several fields that are:

Format Prefix: is 1111 1111.

T: a value of 0 defines that the multicast address is permanently assigned. A value is 1: the multicast address is temporary.

Scope: This is the scope of an IPv6 network used by the router to determine whether the router can forward the traffic. Different values are used:

1: node-local scope

2: link-local scope

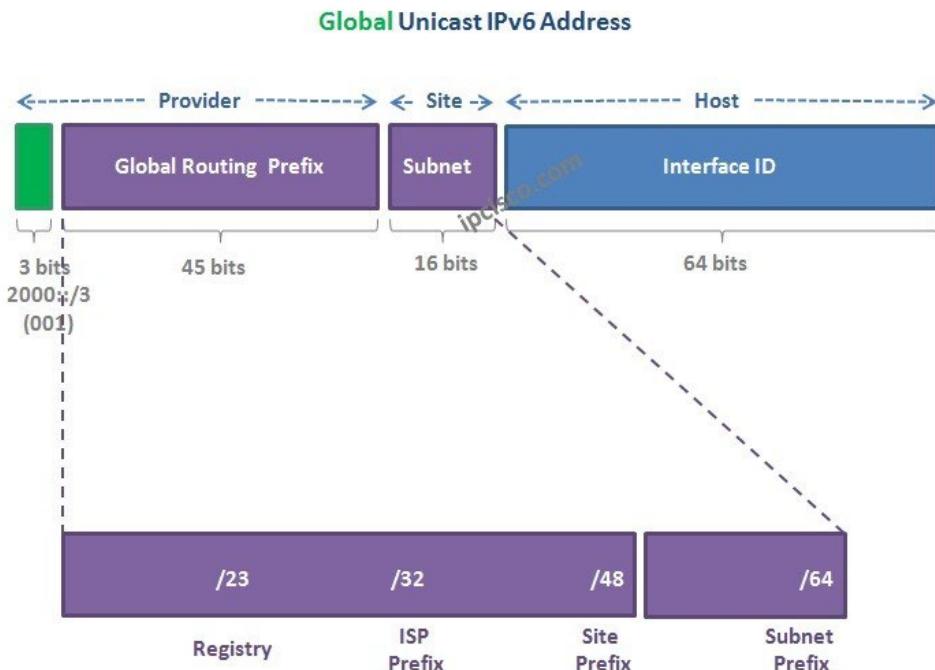
8: organization-local

E: global scope

Group ID: - Identifies the multicast group that is unique within the scope. It contains the reserved addresses from FF01:: to FF0F::.

# Unicast

- Identifies a single interface within the region of the IPv6 network.
- Sends the packets to a single interface when they are addressed to a unicast address.
- Comprises two parts:
  - 64-bit network prefix that is used for routing
  - 64-bit interface identifier that is used for identifying a host computer's network interface



[IPv6 Address Types | Link-Local, Global Unicast, etc.? IpCisco](#)

# Unicast

A multicast address is used to identify multiple interfaces used for one-to-many communication. When multicast addresses are used, packets are sent to all the interfaces using the multicast addresses. A multicast address is never a source address, but always an address that defines a destination. Format Prefix 1111 1111 is used to identify a multicast address. A multicast address always begins with FF.

A multicast address has several fields that are:

Format Prefix: is 1111 1111.

T: a value of 0 defines that the multicast address is permanently assigned. A value is 1: the multicast address is temporary.

Scope: This is the scope of an IPv6 network used by the router to determine whether the router can forward the traffic. Different values are used:

1: node-local scope

2: link-local scope

8: organization-local

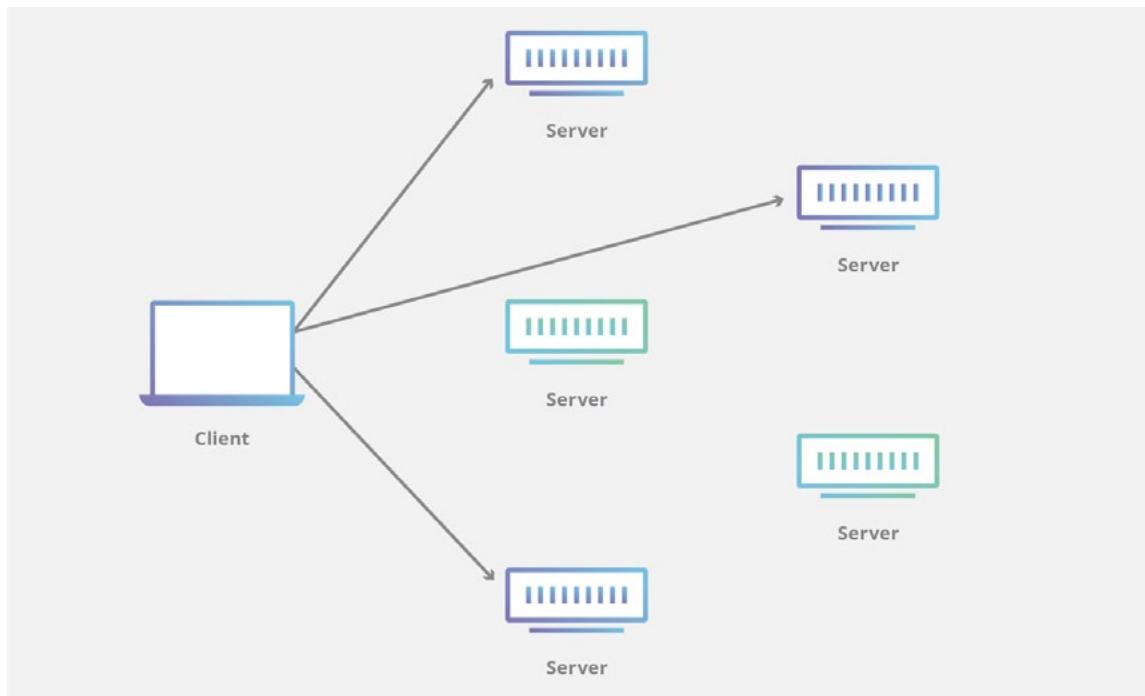
E: global scope

Group ID: – Identifies the multicast group that is unique within the scope. It contains the reserved addresses from FF01:: to FF0F::.



# Anycast

- Identifies multiple interfaces
- Is used for one-to-one-many communication
- Delivers packets to a single interface
- Delivers packets to nearest interface



[What is Anycast? | How does Anycast work? | Cloudflare](#)

An anycast interface is used to identify multiple interfaces. This type of address is used for one-to-one-many communications. The packets are delivered to a single interface from the pool assigned to the anycast address. The packets are delivered to the nearest interface with the anycast address when the delivery is made. When packets are sent to an anycast address, the delivery is made to the nearest interface with the anycast address.

In the current scenario, the anycast addresses are used only for the routers and destination addresses. However, the infrastructure in which the anycast addresses are being used must be aware that there are interfaces with the anycast addresses. If the infrastructure is aware, then the anycast addresses are not used.

Anycast works like the multicast addresses. However, there is a slight difference in the working. An anycast packet is delivered to only one address, the first IPv6 address.

# Link Local

- Is a unicast address
- Is used for communication by nodes that exist on the same link
- Is equivalent to Automatic Private IP Addressing (APIPA) IPv4 address
- Is limited to the local link
- Is used by the Neighbor Discovery processes
- Begins with FE80



A node uses a link-local address to communicate with the neighboring nodes present on the same link. A link-local address is automatically assigned to a node when no other unicast address is assigned.

The link-local address is equivalent to the Automatic Private IP Addressing (APIPA) IPv4 address, which was used in IPv4 when a node did not have an IP address assigned. The link-local represents IPv4 APIPA in IPv6. Two nodes that do not have any other unicast address assigned on the same link can communicate using the link-local addresses.

It is important to note that the link-local addresses are limited to the local link. An IPv6 router cannot forward link-local address traffic outside the link. This means that the link-local traffic is limited within a link.

Neighbor Discovery processes use link-local addresses, and therefore, these addresses are required on a node.

Link-local addresses must always begin with FE80. It has a 64-bit interface identifier, and therefore, the prefix for link-local addresses is always FE80::/64.

Some of the key characteristics of link-local address are:

- It can be used to communicate with the devices on the same link
- Are not routable
- Must be unique on the same link
- Must exist on an IPv6 device

# Loopback

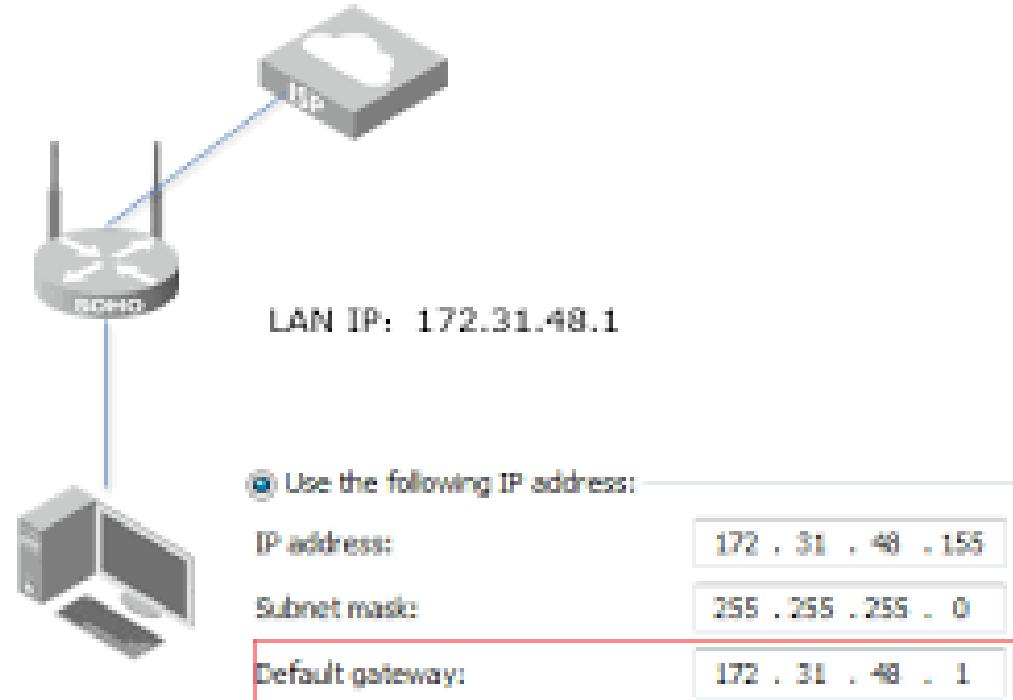
- Denoted with 0:0:0:0:0:0:1 or ::1
- Used for identifying a loopback interface
- Used to enable an interface to send packets to itself
- Is equivalent of IPv4 address, 127.0.0.1

The loopback address is denoted with 0:0:0:0:0:0:1 or double colon ("::")1. It is used for identifying a loopback interface. This address is used to enable an interface to send packets to itself. You can compare this address with IPv4 address, which is 127.0.0.1. This address can never be used to send traffic to a link or a destination address.



# Default Gateway

- Is a node or system that allows the systems from one network to communicate with a node on another network
- Acts as a last resort to the traffic that does not have destination on the same network
- Examples:
  - Home DSL router



If you have ever executed the ipconfig command on Windows or ifconfig command on Linux, you will come across the gateway address. So, what is the importance of this address? When your system is located within a specific network segment, it cannot send the traffic out of the segment. The gateway forwards the packets to the appropriate destination when it is not within the same segment.

When a system needs to send packets to a destination, it first checks for the destination address in its routing table. If it does not find, it sends the packets to the gateway, which then resumes the responsibility of sending the packets to the destination.

If you take the example of a default gateway in your home network, the DSL modem probably has the IP address of 192.168.10.1 or 192.168.0.1. When your system needs to send the packets to an external network, the gateway performs this task.

*TOPIC 3*

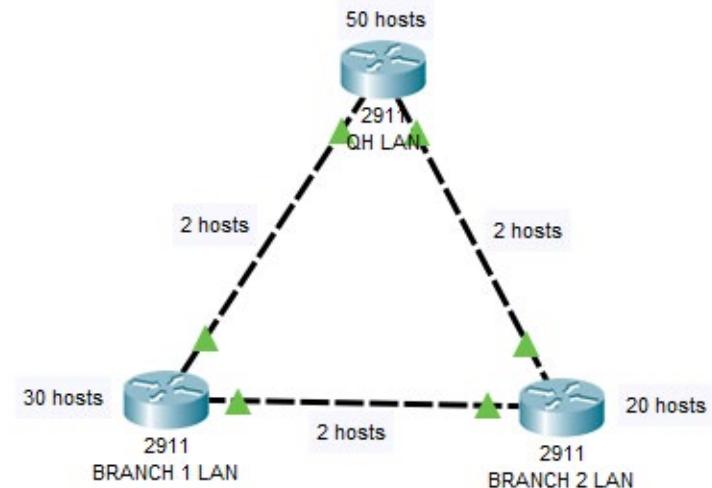
---

# IPV4 SUBNETTING

---

# Classless (Variable-length Subnet Mask)

- Subnet Mask:
  - Determine if a host is on the same network or not
  - Is a 32-bit address
- Variable-length Subnet Mask (VLSM)
  - Allows subnets to be variable in size
  - Allows hosts to be variable in numbers in each subnet
  - Uses only classless routing protocols
  - Uses different configurations for different subnet masks



[Understanding Variable Length Subnet Masks  
\(VLSM\) - Study CCNA \(study-ccna.com\)](http://study-ccna.com)

Before understanding the concept of classless, let's understand the concept of subnet masks. A subnet mask determines the network of a system. It determines whether a system is on the same network or a different network. It is a 32-bit address that is made of ones and zeros. The value of 1 is used as the network prefix, and the value of 0 determines the host. For example, if you /24, the network prefix consists of 24 ones and 8 zeros.

VLSM is a short name for Variable Length Subnet Mask. Consider a scenario of having more than one subnet mask in a single subnet. This is achieved using VLSM, which is subnetting the subnet. VLSM:

- Allows subnets to be variable in size
- Allows hosts to be variable in numbers in each subnet
- Uses only classless routing protocols
- Uses different configurations for different subnet masks

Without the use of VLSM, you will end up wasting IP addresses. For example, if a subnet requires only 10 IP addresses, you will still end up assigning 254, which will waste 244 IP addresses. Using VLSM, you can assign the subnet mask as 255.255.255.240, which will give only 16 IP addresses, out of which 14 will be useful.

VLSM is mainly used with IPv4 public IP addresses.

# Classful

CLASS	LEADING BITS	NET ID BITS	HOST ID BITS	NO. OF NETWORKS	ADDRESSES PER NETWORK	START ADDRESS	END ADDRESS
CLASS A	0	8	24	$2^7$ (128)	$2^{24}$ (16,777,216)	0.0.0.0	127.255.255.255
CLASS B	10	16	16	$2^{14}$ (16,384)	$2^{16}$ (65,536)	128.0.0.0	191.255.255.255
CLASS C	110	24	8	$2^{21}$ (2,097,152)	$2^8$ (256)	192.0.0.0	223.255.255.255
CLASS D	1110	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	224.0.0.0	239.255.255.255
CLASS E	1111	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	240.0.0.0	255.255.255.255

[Introduction of Classful IP Addressing - GeeksforGeeks](#)

This slide displays the classful IP address divided into five classes, namely Class A to Class E. It is important to note that only Class A to C is used. The slide also displays the starting and ending addresses of each class. For example, Class B has a 128.0.0.0, and the ending address is 191.255.255.255.

There are fewer networks in Class A but more hosts per network. Similarly, Class C has fewer networks, but there are more hosts per network. The slide also displays the number of bits used for networks and hosts. Class A has only 8 bits for the network, whereas Class C has 24 bits for networks. In the Addresses Per Network column, the number mentioned in the parentheses is the number of hosts per network. You must subtract two addresses from the total number of hosts, 0.0.0.0 and 127.0.0.1, as they cannot be allocated.

# Classless Inter-Domain Routing (CIDR) Notation

- Is used for allocation of IP addresses
- Is based on VLSM
- Breaks the IP addresses into two parts:
  - Network address: Is used as a prefix
  - Remaining address: Is used as a suffix with the number of bits remaining in the address
- Overall improves the efficiency of IPv4 allocation without wasting IP addresses

The CIDR notation is used for allocating IP addresses without wasting too many IP addresses. In the previous slide, you look at the VLSM method that reduces wastage by allocating only the required IP addresses. You also looked at the example of 255.255.255.240, which will allocate only 16 IP addresses. If you do not use VLSM, the total IP address allocated will be 256, which means you will waste 246 IP addresses if you need just 10 of them. So, in a nutshell, CIDR uses the VLSM method for IP address distribution.

CIDR breaks the IP address into two parts:

Network Address: This is used as a prefix

Remaining address: This is used as a suffix with the number of bits remaining in the address

For example, you have 192.168.1.0/24 – you get a total of 256 IP addresses. However, you have to remove two IP addresses and, therefore, are left with 254.

Let's simplify the concept of CIDR. You know that there are three classes of IP addresses:

- Class A - 16 million hosts
- Class B - 65,535 hosts
- Class C - 254 hosts

Suppose you need to use a class B IP address but require only 5000 IP addresses. In this scenario, you would waste nearly 60000 IP addresses. So, what is the solution? You use the CIDR notation to reduce the wastage of the IP address. With the CIDR notation of /19, you will get 8192 IP addresses. Even though you still waste a little more than 3000 IP addresses, it is still better than wasting 60000.

CIDR Block Size	Exponential Notation	Number of Addresses
/24	$2^8$	256
/23	$2^9$	512
/22	$2^{10}$	1,024
/21	$2^{11}$	2,048
/20	$2^{12}$	4,096
/19	$2^{13}$	8,192
/18	$2^{14}$	16,384
/17	$2^{15}$	32,768
/16	$2^{16}$	65,536

[How to Choose the CIDR Block for Your VPC | MuleSoft Blog](#)



*TOPIC 4*

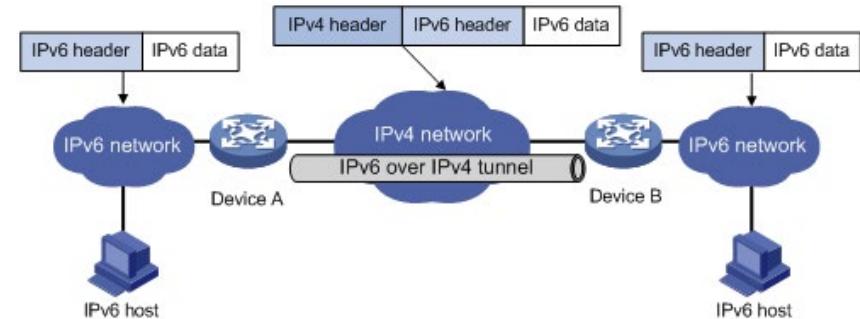
---

# IPV6 CONCEPTS

---

# Tunneling

- Encapsulates the IPv6 packets with an IPv4 header
- Allows the IPv6 packets to be sent to an IPv4 network.
- Sets the Protocol field to 41 indicative of an encapsulated IPv6 packet
  - Source field: IPv4 address
  - Destination field: IPv4 address
- Need to configure the tunnel endpoints manually or automatically.



[IPv6 over IPv4 tunneling \(hpe.com\)](http://hpe.com)

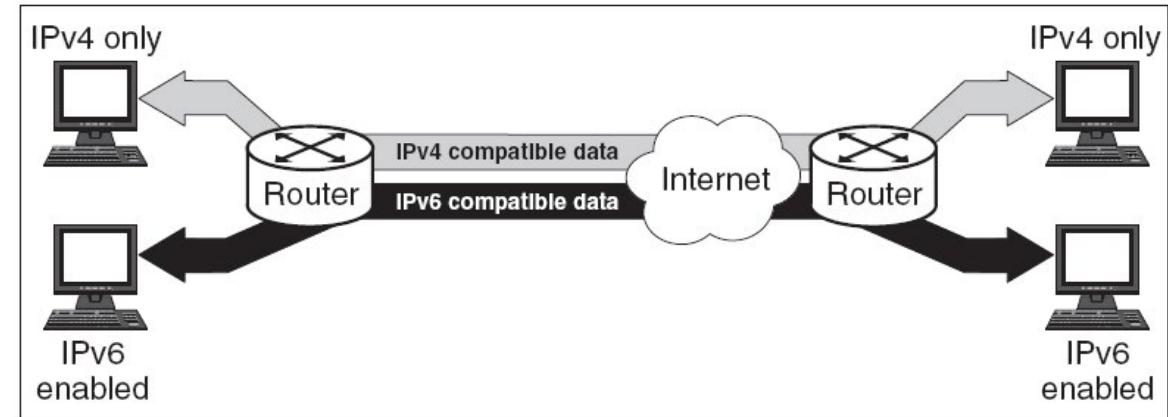
There may be a possibility when you need to send the IPv6 packets to the IPv4 network, which does not understand the IPv6 format. This makes communication between both networks rather difficult. You can use the tunneling method that encapsulates the IPv6 packets into the IPv4 header to resolve this issue. The IPv6 packets can be delivered to the IPv4 network with this mechanism.

In the tunneling method, the IPv4 header adds another IPv6 header that contains the IPv6 information. The Protocol field is marked with the value of 41, indicating an encapsulated IPv6 packet. However, the Source and Destination fields are marked with the IPv4 fields.

At both ends of the tunnel, you have the endpoints. Each of the endpoints must be configured manually or automatically.

# Dual Stack

- Is a migration strategy
- Allows the devices and applications to be configured with IPv4 and IPv6
- Requires gradual movement to the IPv6



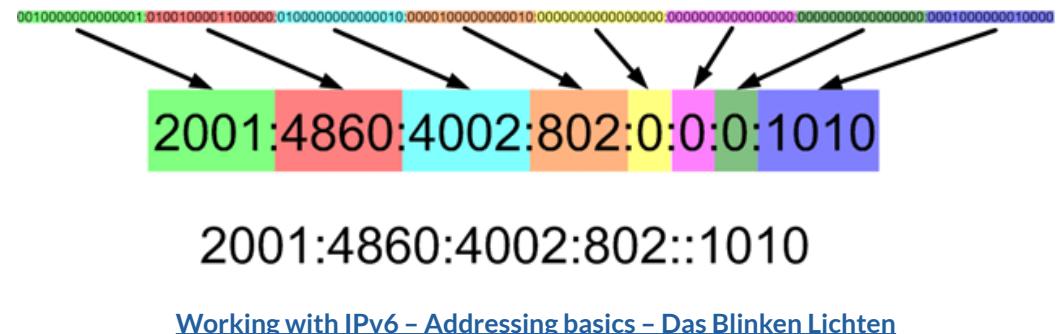
[What Is IPv4 & IPv6 Dual Stack and MPLS Technique? \(cables-solutions.com\)](http://cables-solutions.com)

The dual-stack is an IPv4 to IPv6 migration strategy. Consider that you have an IPv4 network. You want to migrate it to IPv6. There are two options – you can scrap the IPv4 network and start with IPv6. On the other hand, you can migrate one application or system at a time. In the second case, you need to have IPv4 and IPv6 IP addresses on the systems and applications.

You can continue to migrate one by one, and eventually, in the end, all systems and applications will be moved to the IPv6 stack. However, the important point to note is that for some time, both IPv4 and IPv6 will continue to exist in parallel. This is probably the best migration strategy without impacting the network functionality.

# Shorthand Notation

- Leading zeros are removed in a 16-bit block.
  - Each block must have a minimum one digit.
  - Original address:
    - 21DA:00D3:0000:2F3B:02AA:00FF:FE28:9C5A
  - With leading zeros removed:
    - 21DA:D3:0:2F3B:2AA:FF:FE28:9C5A
  - Zeros in contiguous sets can be removed and replaced with “::” (double colon).



All leading zeros in the hexadecimal format can be removed from the address. Each set of 16-bit blocks that contains leading zeros can be compressed into a format that does not require leading zeros. This means that the address can be compressed into a smaller hexadecimal format.

It is important to note that each 16-bit block must have a minimum of one digit. If there is no digit, the leading zeros cannot be removed.

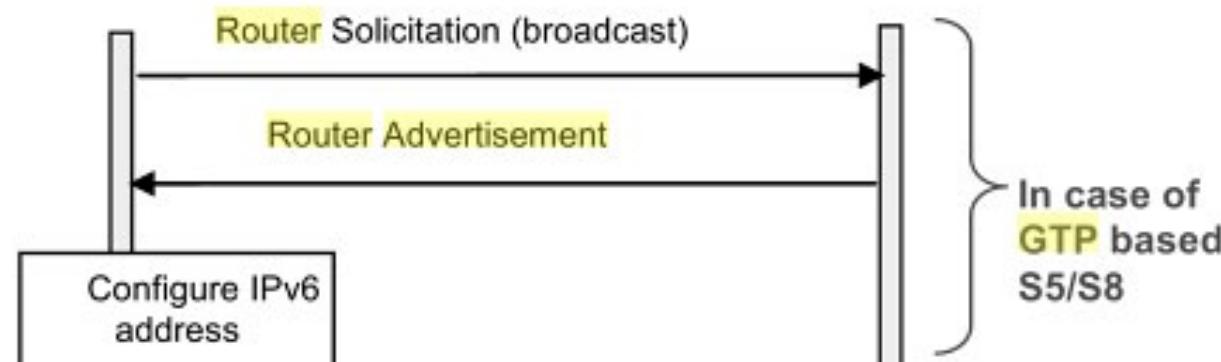
When leading zeros are removed, they are shown in the compressed format. In the above example, 21DA:D3:0:2F3B:2AA:FF:FE28:9C5A shows a compressed format. The third set of 0000 is compressed into a single 0, and the address then shows :0: as a replacement to the 0000. A single zero is shown.

When zeros are in the continuous sets, you can replace them with the double colon ("::"). However, it is important to note that zeros can be compressed only once in an address. For example, if you have an address that is 21DA:0:0:2F3B:02AA:00FF:FE28:9C5A, you can write it like 21DA::2F3B:02AA:00FF:FE28:9C5A.

# Router Advertisement

- Is sent by the router to provide network ID to the hosts
- Is a response to Router Solicitation message

If you wants UE to configure an IPv6 address

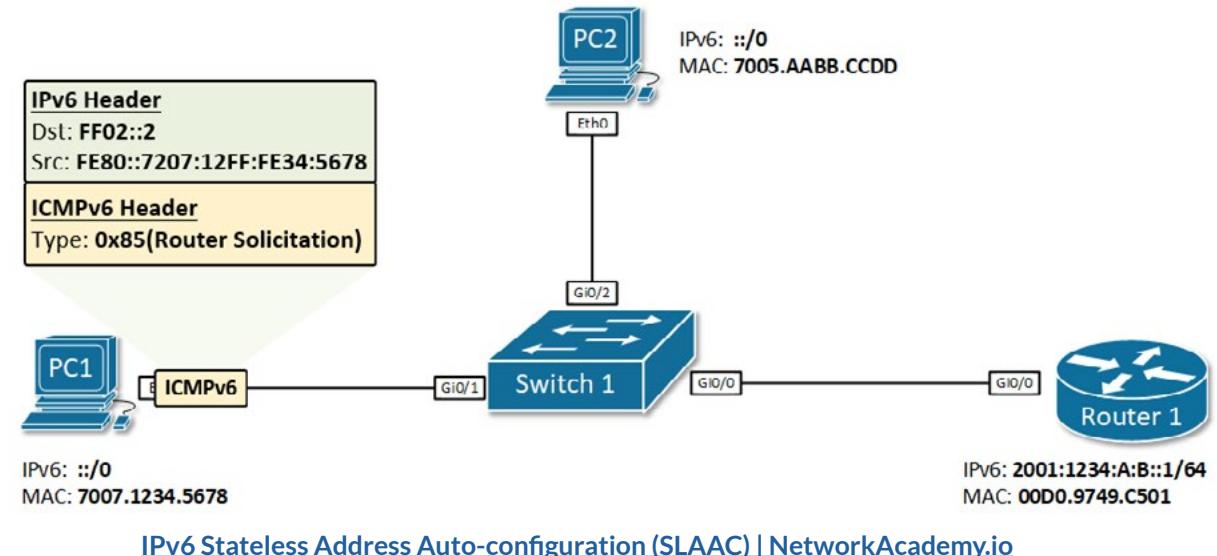


[Landslide:Router advertisement message in GTP flow between PGW user node and SGW user node \(spirent.com\)](#)

A router performs a Router Advertisement to provide the network ID to the hosts on the network. It is sent in the form of a packet. However, the router itself does not initiate this process, which a host initiates on the network. The host sends the Router Solicitation (RS) message to all routers and receives the Router Advertisement (RA). You will learn about the detailed process on the next slide.

# Stateless Address Autoconfiguration (SLAAC)

- Assigns a network device with a link-local unicast address and a global unicast address
- Does not require a DHCP
- Uses the prefix information from the router and appends the MAC address of the device using NDP



In the previous slide, you learned about the RA message. Now, let's look at SLAAC, a stateless Address Autoconfiguration that assigns a network device with a link-local unicast and a global unicast address. So, how does SLAAC help – it removes the dependency of having a DHCP server to lease the IP addresses.

Let's quickly look at the process:

As the first step, a host generates a link-local address.

- The host then sends a Router Solicitation message in a multicast message to all routers.
- Upon receiving the multicast message, the router responds with the prefix information using the Router Advertisement (RA), also a multicast message.
- After receiving the prefix information, the host generates the IP address, which is an IPv6 address. It uses the prefix and its own MAC address.
- The host then performs the duplicate address detection (DAD) process.
- If there is no positive outcome of DAD, then the newly generated IP address is marked as tentative.
- Finally, the address is allocated to the host.

In case of a situation, if there is no response from routers on the network, the host attempts to look for a DHCP Server.



*TOPIC 5*

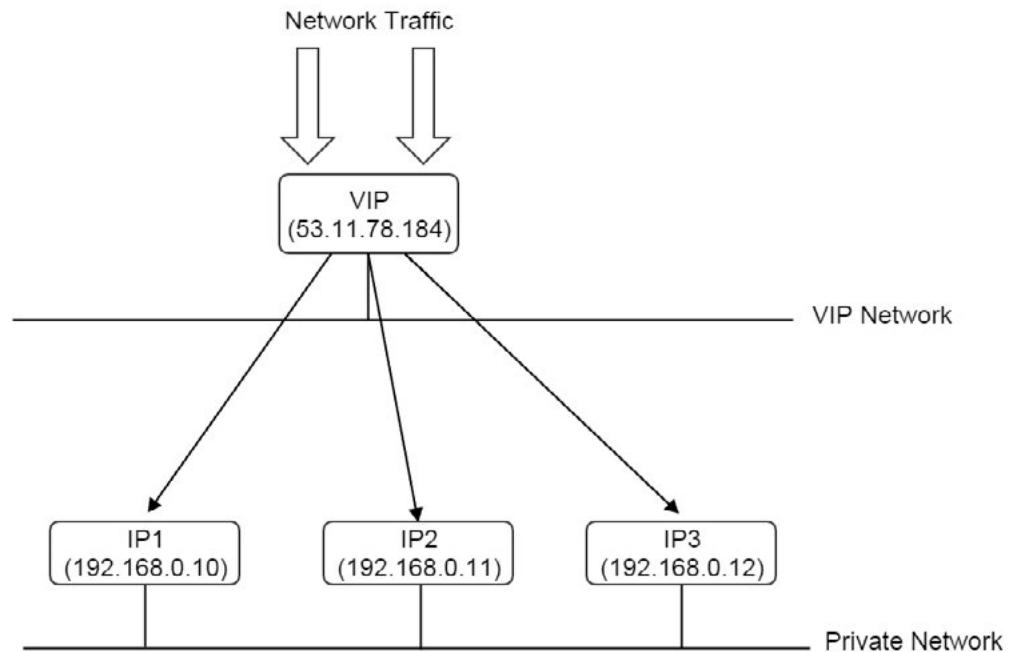
---

# VIRTUAL IP (VIP)

---

# Virtual IPs (VIPs)

- Is substitution of a public IP address with private IP addresses of a NIC
- Is the public IP address that is NOT assigned to the NIC
- Can be configured with NAT using routers or firewall



[Virtual IP Address – zstack 0.6 documentation \(zstackdoc.readthedocs.io\)](https://zstackdoc.readthedocs.io)

A virtual IP can be a public IP address not assigned to the physical NIC in a system or a networking device but is used to represent the system. When the traffic is sent to the public IP address, it is further distributed to the actual IP addresses assigned to the physical NIC. This is an example of NAT that uses a public IP address for several private IP addresses.

Another great example of a virtual IP can be the IP address of the load balancer. Consider that you have configured a load balancing cluster. Two servers are configured with a software load balancer. Each server has its IP address, and the load balancer has another IP address. When the clients connect, they use the load balancer's IP address, the virtual IP address.



***TOPIC 6***

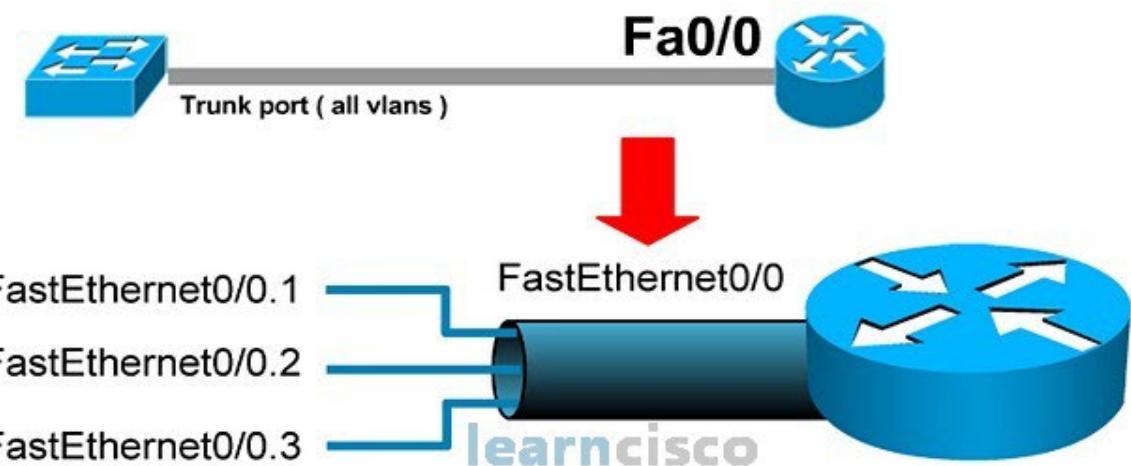
---

# SUBINTERFACES

---

# Subinterfaces

- Divide a single physical NIC into two or more interfaces
- Is a virtual interface that is part of the physical interface
- Is configured like a physical interface
- Example:
  - A Cisco router with one physical NIC that is divided into two subnets for routing the data



[Inter VLAN Routing | ICND1 100-105 \(learnCisco.net\)](#)

When a physical NIC interface is divided into multiple interfaces, it is the subinterfaces you have created. It is possible to configure multiple subinterfaces on a physical interface. For example, you have a router with one NIC but must configure three subnets. You can create subinterfaces. If the interface is FastEthernet0/0, the subinterfaces would be like:

- FastEthernet0/0.1
- FastEthernet0/0.2
- FastEthernet0/0.3

# Summary



Public vs. private



IPv4 vs. IPv6



IPv4 Subnetting



IPv6 Concepts



Virtual IP (VIP)



Hi, welcome to COMPTIA Network+ Course

In this, we will talk about:

- Public vs. private
- IPv4 vs. IPv6
- IPv4 Subnetting
- Public vs. private
- IPv4 vs. IPv6
- IPv4 Subnetting





*NEXT TOPIC*

---

# COMMON PORTS AND PROTOCOLS

---

Lesson

# 5

# Common Ports and Protocols

- 1 — Welcome to the lesson 5 of Module 1. In this lesson, you will learn about the:
- 2 — Various networking protocols and their ports.



Network Fundamentals

# AGENDA



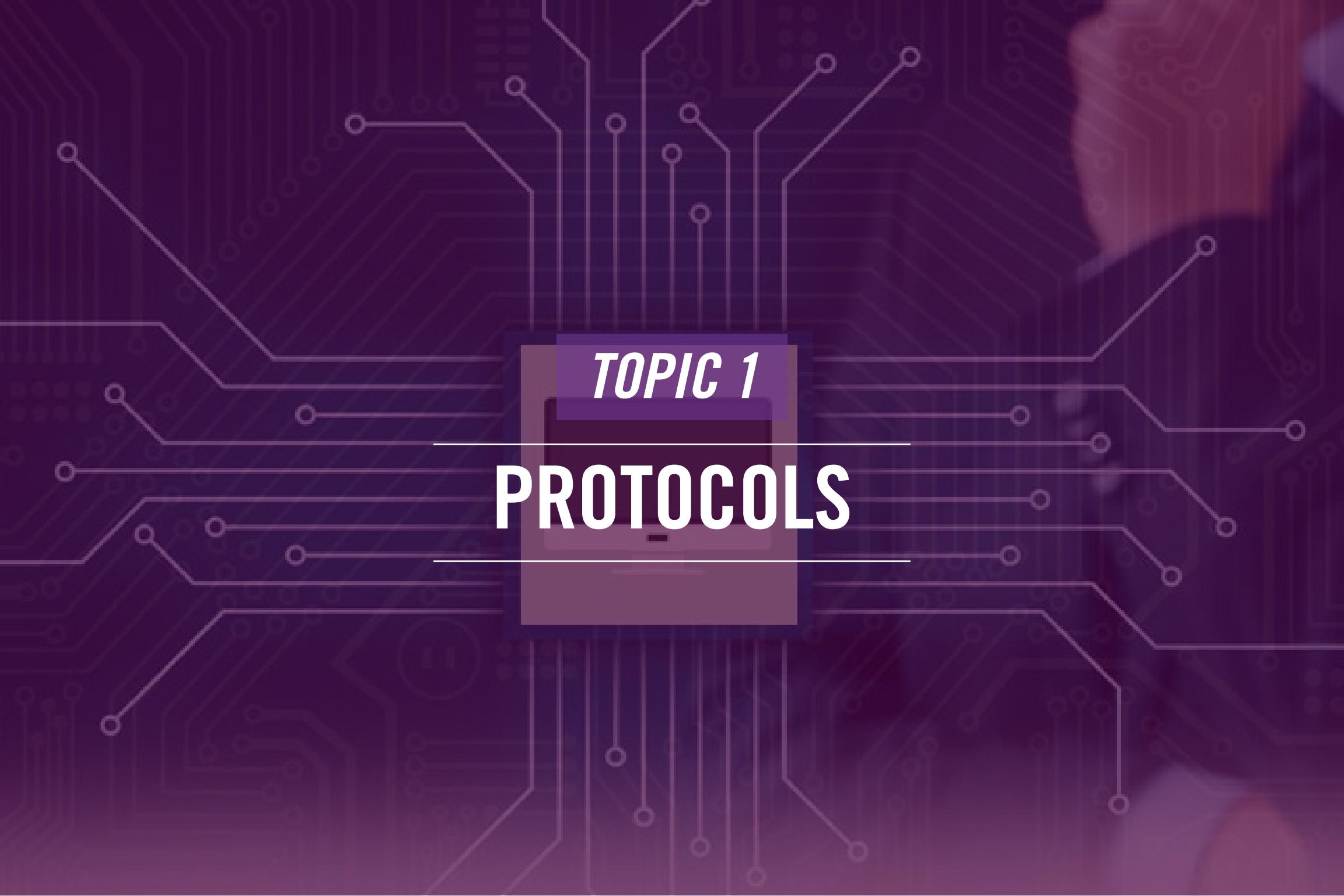
## Protocols



Hi, welcome to COMPTIA Network+ Course  
In this, we will talk about:

- Protocols



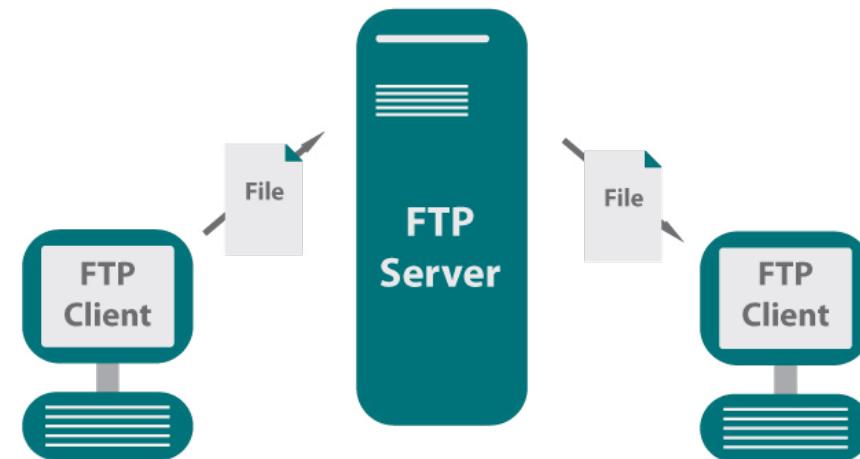


*TOPIC 1*

# PROTOCOLS

# File Transfer Protocol (FTP)

- Let's you transfer files from one system to another system where:
  - One system acts as an FTP server
  - One system acts as a client
- Allows users to access files and directories depending on permissions
- Uses ports 20 and 21



[What is file transfer protocol \(FTP\)? - Ipswitch](#)

File Transfer Protocol (FTP) is a protocol that allows a user to connect to a server and upload or download files. It allows you to transfer files to or from a server. You have a server that acts as an FTP server. The FTP clients can be a command line or a utility with a graphical user interface (GUI).

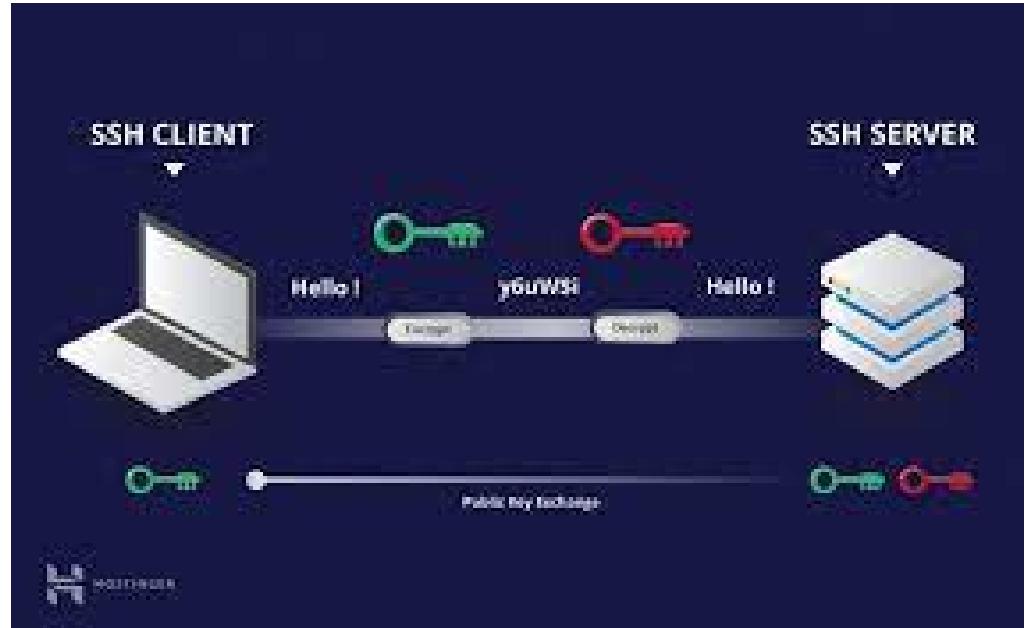
The FTP server can be configured with authentication or allow anonymous authentication. The FTP server contains the directories and files with permissions set on them. The users are granted permissions on these directories and files.

FTP is now rarely used because of its insecure communication. It is inherently an insecure protocol that sends the information in cleartext format.

FTP uses ports 20 and 21. Port 20 is used for data transfer. Port 21 is used for establishing a connection between the server and the client.

# Secure Shell (SSH)

- Is a protocol that is used for remote connectivity
- Replaces telnet
- Uses an encrypted channel to connect with the remote host
- Uses TCP port 22



[Secure Shell \(SSH\) - CyberHoot](#)

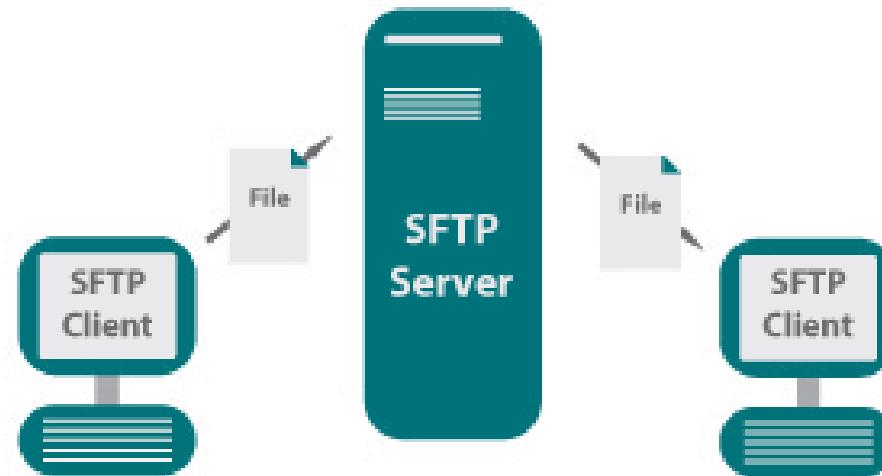
Often, you need to work with remote Linux or UNIX servers. You can use the Secure Shell (SSH) protocol to establish a remote connection with these servers. You need to set up an SSH server on the server you want to connect. You also need to have the SSH client on your system to establish the connection.

When you use SSH, it establishes an encrypted channel between the server and the client. Once the connection is established, you can manage the system, transfer files, or do other administrative tasks.

SSH uses TCP port 22.

# Secure File Transfer Protocol (SFTP)

- Is used to transferring files over an encrypted connection
- Uses SSH to encrypt the connect
- Uses TCP port 22 – same as SSH

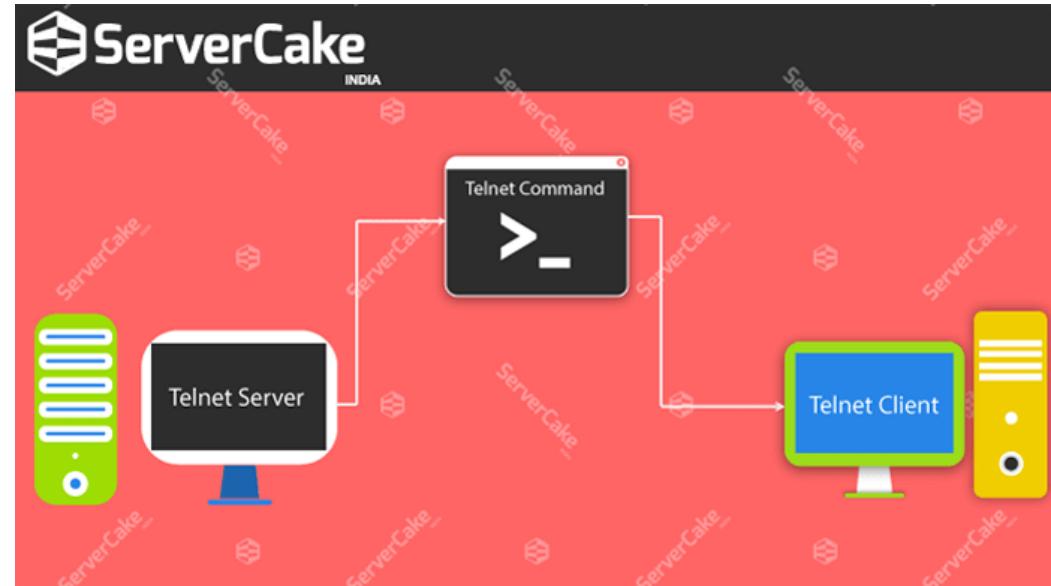


[What is SFTP Server - Ipswitch](#)

You had just learned about FTP, an insecure protocol that used to be widely used for transferring files. It was used on internal networks and over the Internet by several organizations. However, its use has decreased over the years because of its inherent vulnerabilities. SFTP or Secure File Transfer Protocol is now being used. It serves the same purpose as FTP, but instead of sending information in a cleartext format, it encrypts the channel for file transfer. SFTP uses SSH for encrypting the connection. Because it uses the SSH protocol, it uses the same TCP port 22.

# Telnet

- Allows a user to connect to remote system
- Works in the client/server model
- One system acts like a telnet server
- One system works like a client
- Uses TCP port <sup>23</sup>



[What is Telnet Command - ServerCake India Webhosting](#)

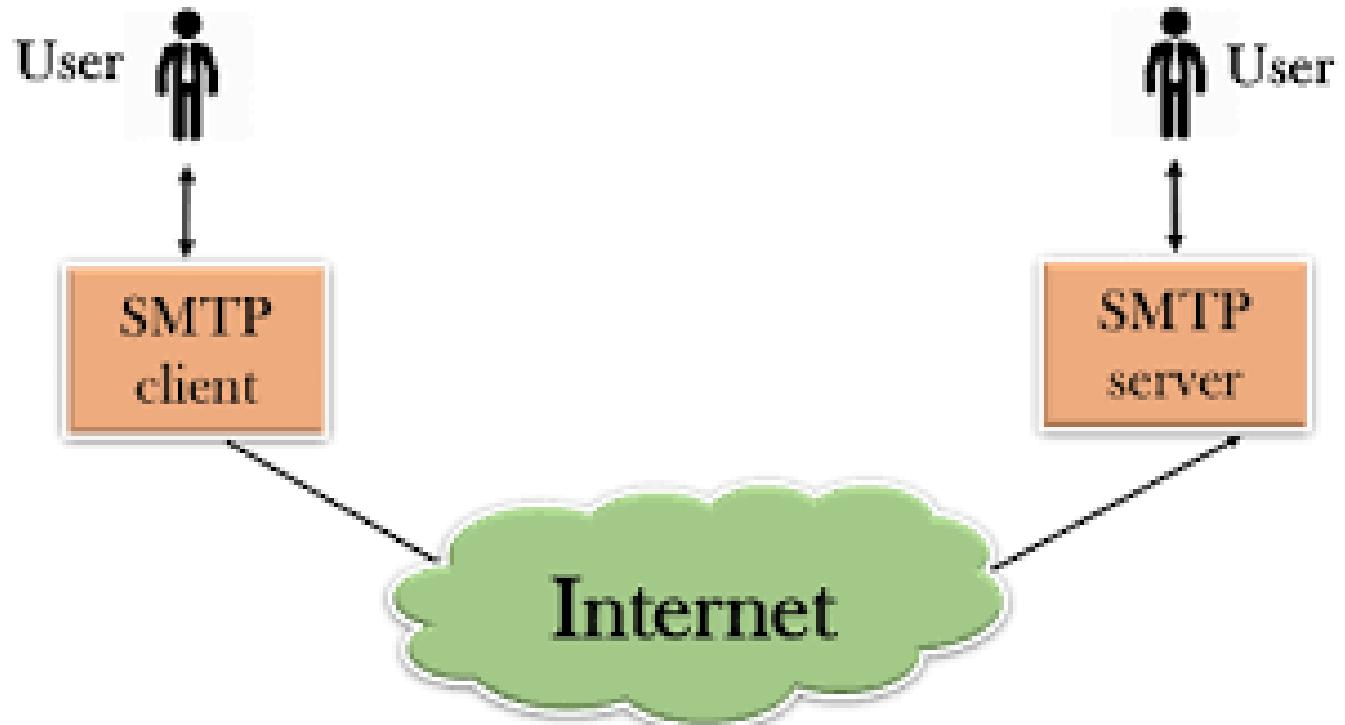
Telnet, just like SSH, is used for remotely managing the Linux and Unix system. However, like FTP, telnet is also an insecure protocol that shares information in cleartext format. It works in the client/server model – you need to set up a telnet server and a client.

Because of telnet's insecurities, it was possible to sniff or capture the information from a session between a client and the server. Therefore, over the years, telnet has been replaced by SSH.

Telnet uses TCP port 23.

# Simple Mail Transfer Protocol (SMTP)

- Is used to send emails
- Uses TCP port 25

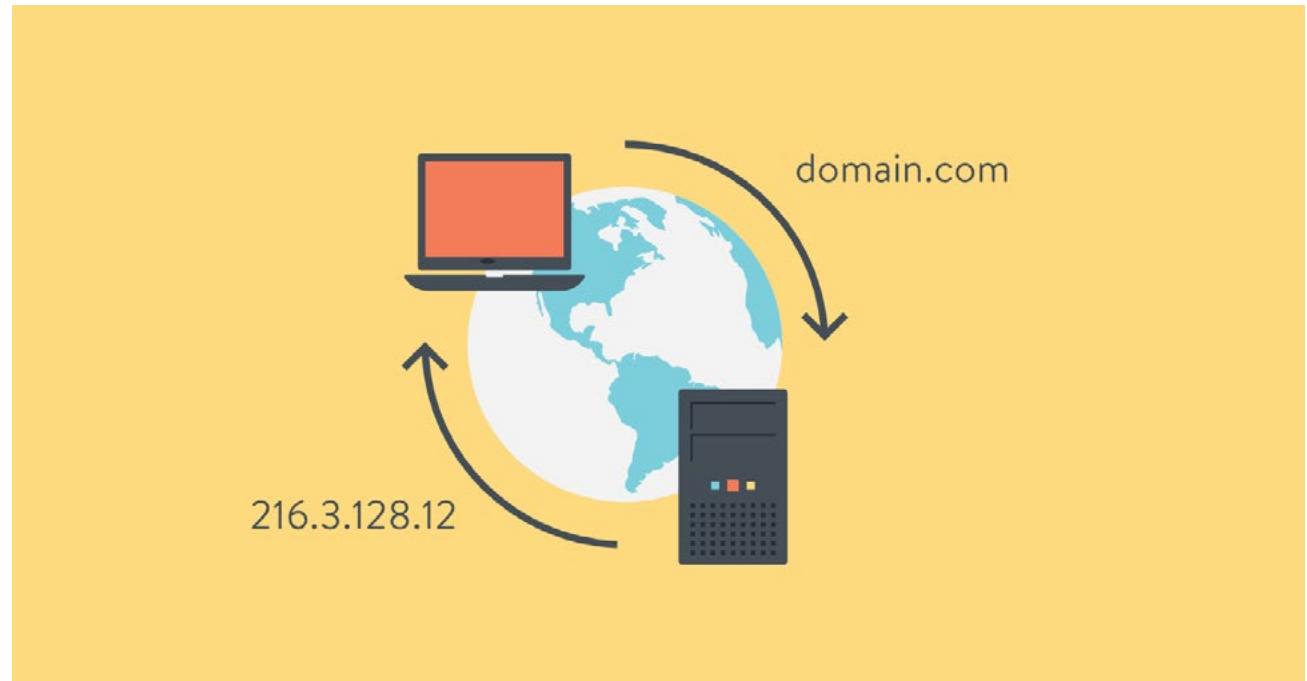


[SMTP or IMAP: What's the Difference? \[Bonus: What is POP3?\]](https://www.socketlabs.com) (socketlabs.com)

Simple Mail Transfer Protocol or SMTP is used for sending emails. The SMTP protocol sends the email to the destination email server when a user is sending an email. The recipient may be using another protocol, such as POP3, to download email from his email server.  
SMTP uses TCP port 25.

# Domain Name System (DNS)

- Is used for domain name resolution
- Uses TCP and UDP port 53

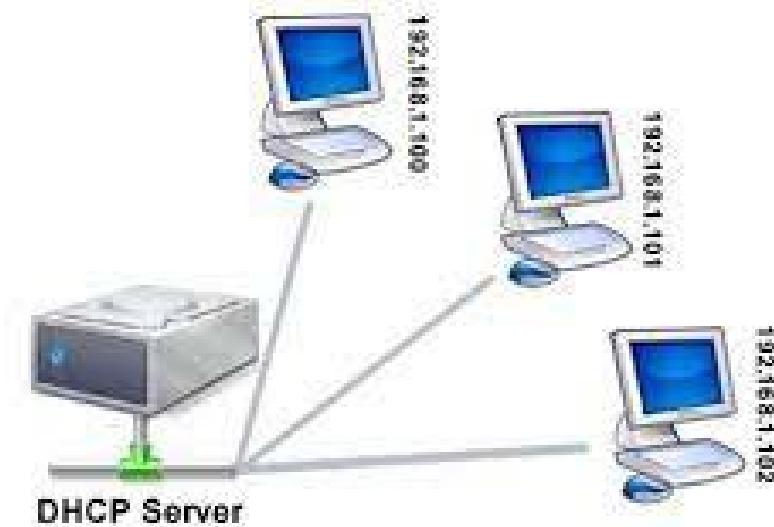


[What is DNS? Domain Name System Explained \(kinsta.com\)](https://kinsta.com/dns-explained/)

Domain Name Service or DNS is a protocol used for name resolution. Think of the Internet if you had to remember several IP addresses to browse various Websites. It won't be possible. DNS makes the job easy. You need to type the Website or domain name, and then DNS would resolve the domain name or Website name to the correct IP address and make it appear in your Web browser.  
DNS uses TCP and UDP port 53.

# Dynamic Host Configuration Protocol (DHCP)

- Is used for leasing IP addresses to the networked systems and devices
- Can be configured in various network devices, such as wireless routers
- Uses UDP port 67 and 68



[Overview of Dynamic Host Configuration Protocol \(DHCP\) for Beginners \(whatismyipaddress.com\)](http://whatismyipaddress.com)

Dynamic Host Configuration Protocol or DHCP is used for leasing IP addresses to the networked systems. You can assign IP addresses manually or using DHCP. It is easy to assign IP addresses manually when you have a small network of 5-10 systems. However, when dealing with hundreds or even thousands of systems, it becomes challenging to manage IP address assignments manually. In such a case, DHCP comes handy.

It can assign an IP address, subnet mask, gateway, and DNS information to the client systems on the network.  
DNS uses UDP ports 67 and 68.

# Trivial File Transfer Protocol (TFTP)

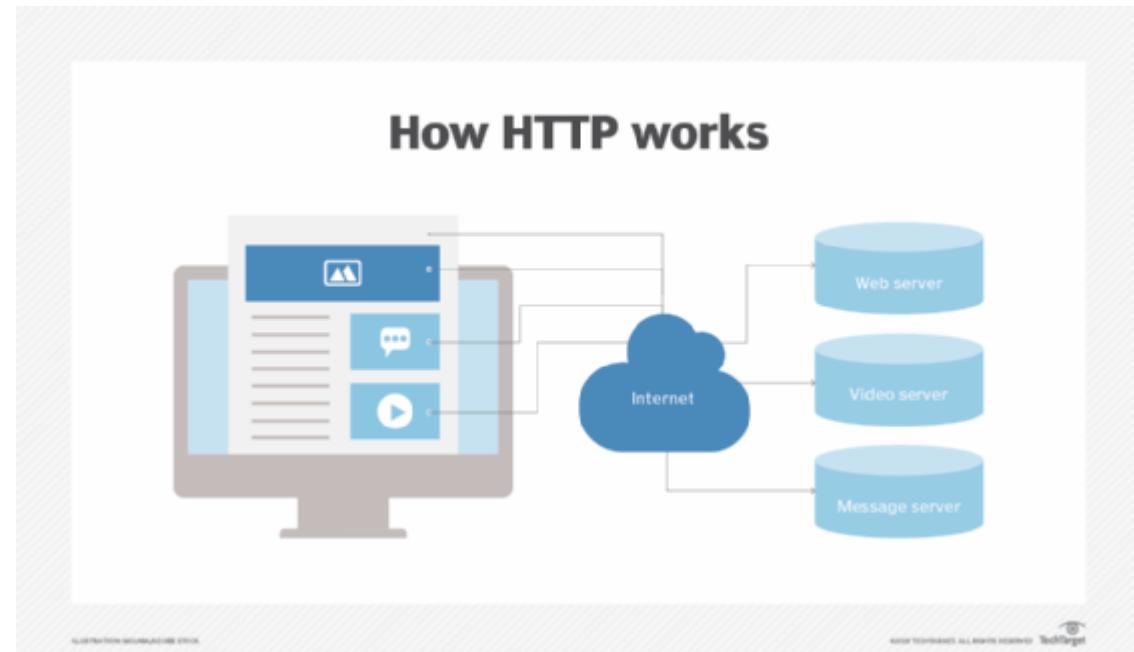
- Works like FTP but without providing the capability of directory browsing
- Is mainly used for sending and receiving files
- Requires the use of exact file name to be downloaded
- Uses TCP port 69



Trivial File Transfer Protocol or TFTP works just like an FTP server. However, there are a few exceptions though. It does not have directory browsing capabilities. This means that the user cannot connect to a TFTP server and start browsing. You need to know the IP address and name of the file you want to download from a TFTP server. You can send and receive files from the TFTP server. For downloading or receiving the files, you need to provide the URL along with the file name. TFTP is primarily used with the network devices for uploading the firmware or configuration files. TFTP uses TCP port 69.

# Hypertext Transfer Protocol (HTTP)

- Is used for Web browsing
- Establishes a connection between the Webserver and the Web browser
- Uses TCP port 80



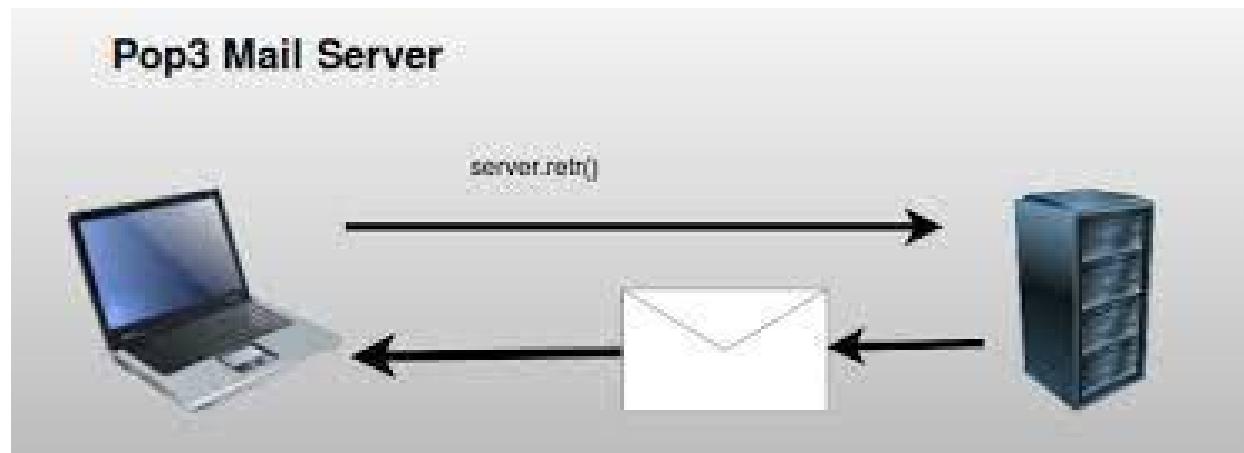
[What is HTTP and how does it work? Hypertext Transfer Protocol Definition \(techtarget.com\)](#)

When browsing a website, you are most likely using the HTTP protocol, primarily used with static websites. The HTTP protocol establishes a connection between the Webserver and the Web browser. It makes it possible for a user to navigate the website. For example, if a link is given on the website when a user clicks on the link, HTTP makes it possible to provide the same webpage to the user's Web browser.

It is important to note that most websites now use HTTPS, which you will learn shortly.  
HTTP uses TCP port 80.

# Post Office Protocol v3 (POP3)

- Is used to download emails from the server to the client
- Allows the clients to store emails locally but deletes from the server
- Uses TCP port 110



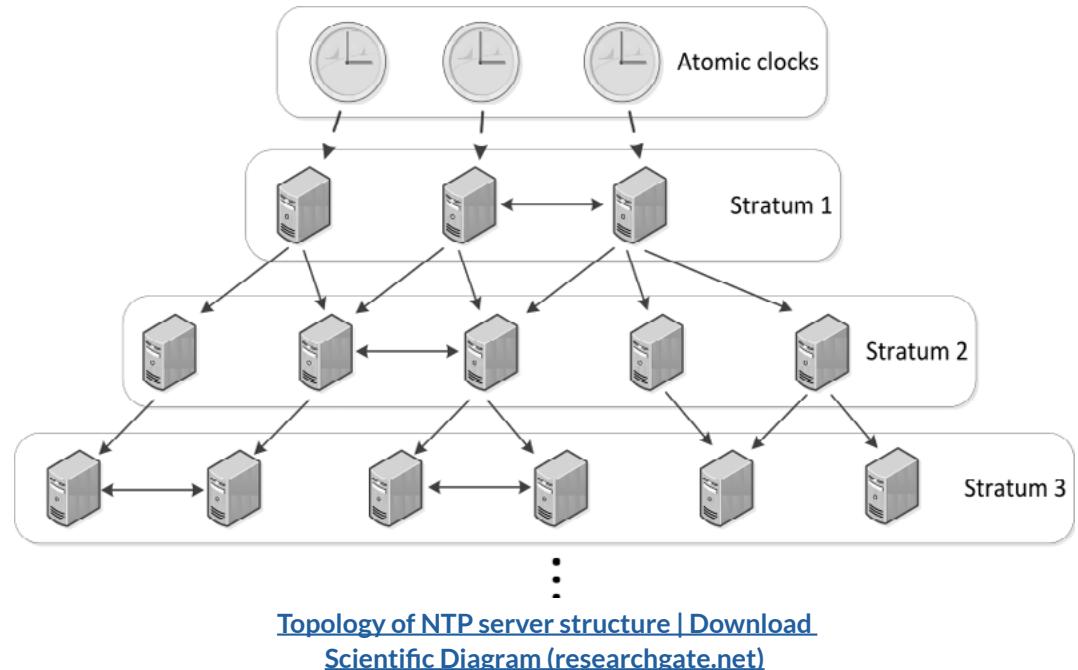
[Read Email, pop3 - Python Tutorial \(pythontutorial.com\)](http://Read Email, pop3 - Python Tutorial (pythontutorial.com))

POP3 or Post Office Protocol version 3 is used to download emails from a messaging server. It is mainly functional between the recipient's messaging server and the client. When an email is delivered on the recipient's messaging server, the messaging client at the user's end can be configured to download emails using POP3. Of course, the messaging server also needs to be configured with POP3.

When the emails are downloaded at the client's end, they are deleted from the server. This means that the messaging server no longer retains the emails. When using POP3, you cannot selectively download emails from the messaging server. All emails get downloaded on the client, and the server no longer retains any email. POP3 uses TCP port 110.

# Network Time Protocol (NTP)

- Is used to synchronize the system clocks to a single time source
- Uses UDP port 123



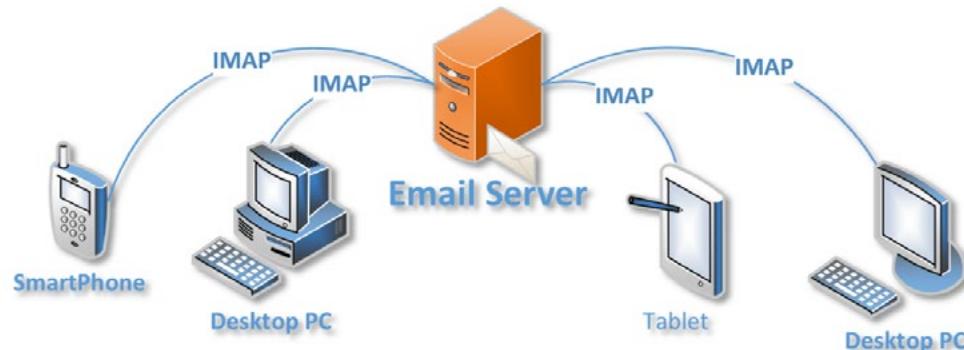
Have you ever wondered how your system always displays the correct time of the day? This is possible because of the Network Time Protocol (NTP). There can be a hierarchy of NTP servers that are synchronizing with each other. Your organization can also configure an NTP server internally and configure the client systems and servers to synchronize with it.

The internal NTP server can be configured to synchronize with some external NTP servers, then synchronized with the atomic clocks. In this manner, a hierarchy of NTP servers is built.

NTP uses UDP port 123.

# Internet Message Access Protocol (IMAP)

- Is used to synchronize the emails on the devices
- Does not delete the message from the server after synchronization
- Uses TCP port 143



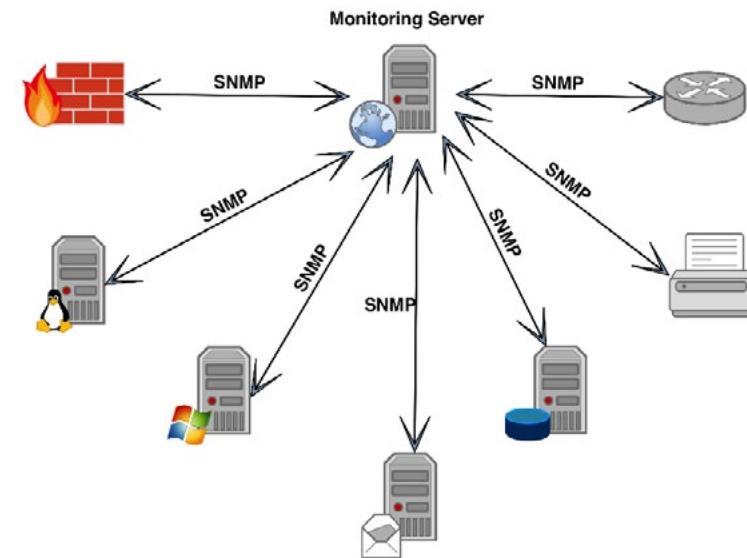
[What is IMAP? And How Can it Help Me Manage My Email? - Ask Leo!](#)

Internet Message Access Protocol or IMAP is a protocol that allows a client to access emails on the server. Unlike POP3, IMAP can download emails to more than one client but retains the emails on the server. This means that even though the message is downloaded on one or more clients, it is still retained on the server. One of the good features of IMAP is that you can manage your messages on the server. You can delete, create, or even rename emails, which was not possible with POP3. Any changes to the email messages, such as deleting a few, are synchronized with the clients. Similarly, any changes to the messages on the client are also synchronized with the server.

IMAP uses TCP port 143.

# Simple Network Management Protocol (SNMP)

- Is a network monitoring protocol
- Can gather information from various network devices
- Requires the agents to be installed on the devices
- Uses Network Management System (NMS) to question the agents
- Uses Management Information Base (MIB) to question agents
- Uses UDP port 161 and 162



[Introduction Simple Network Management Protocol \(SNMP\) \(ozeki.hu\)](http://www.ozeki.hu)

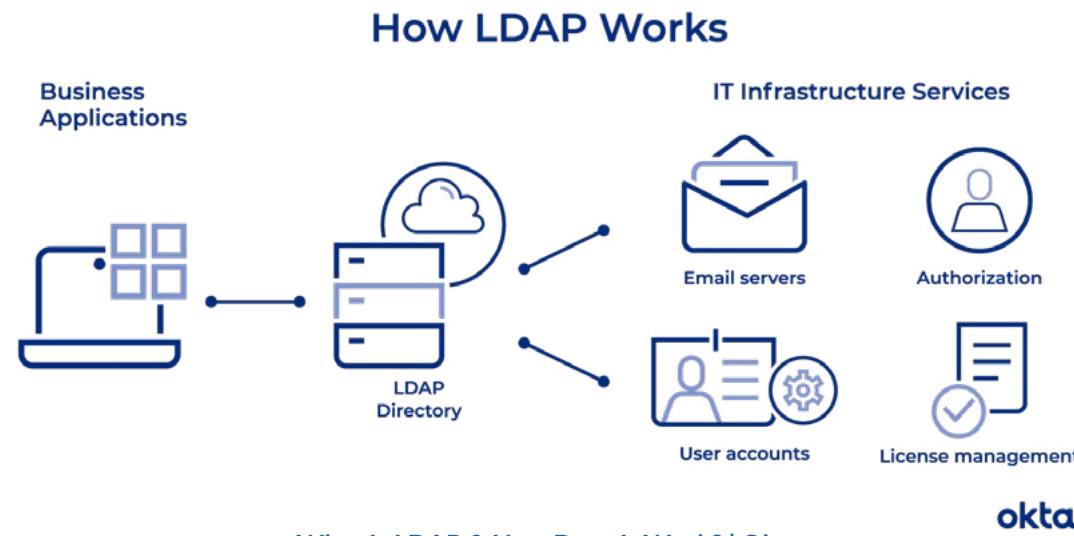
When working in a network environment, you would have several or even hundreds of network devices, such as switches, firewalls, and routers. You need to know when they become non-functional or any problem, such as resource crunch, takes place. You can use the SNMP protocol to do the same.

You have agents that are installed and configured on networked devices. They are responsible for reporting any issue to the Network Management System (NMS), which uses the Management Information Base (MIB) to question the agents. MIBs contain pre-defined parameters that are used to question the agents. If there is an issue with one of the networked devices, its agent quickly informs the NMS by sending an alert.

SNMP is currently in version 3 and uses the UDP ports 161 and 162.

# Lightweight Directory Access Protocol (LDAP)

- Is a centralized library database to keep track of network resources
- Is the base of Microsoft Active Directory
- Uses TCP port 389



If you have ever worked in a Windows domain, you are authenticated through a centralized server called domain controller, which runs Active Directory. You can think of the Active Directory as a centralized repository that contains a lot of things, such as user and group accounts and registered client systems and servers.

Active Directory uses LDAP as the base that helps it track all the systems, users, and groups that exist. Of course, an authentication mechanism is built in to ensure that the users are correctly authenticated.

Authentication is not the only purpose of LDAP. It also gets integrated with the applications. For example, you develop an application that requires user authentication. Now, either you can build the user database within the application or integrate LDAP and use the existing userbase.

LDAP uses TCP port 389.

# Hypertext Transfer Protocol Secure (HTTPS)[SSL]

- Is a combination of HTTP and SSL to securing online Web browsing and transactions
- Uses TCP port 443

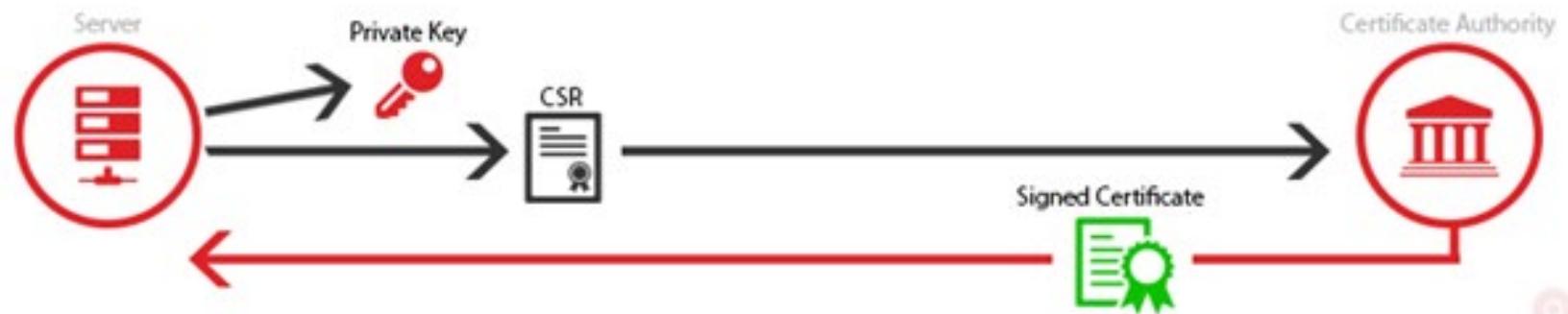


[SSL Handshake explained. If you have ever browsed an HTTPS URL... | by Kasun Dharmadasa | Medium](#)

You earlier learned about the HTTP protocol. HTTPS is also HTTP with SSL. It is, what you can consider, a secure version of HTTP. With the HTTP, the information exchange between the Web browser and the Webserver was not secure and was done in cleartext. HTTPS removes this vulnerability and exchanges the information between the parties in an encrypted format. HTTPS becomes handy when conducting an online e-commerce transaction or filling out a form. HTTPS uses TCP port 443.

# HTTPS [Transport Layer Security (TLS)]

- Is an encryption protocol for securing the Web activities like Web browsing
- Use X.509 certificate and asymmetric encryption
- Authenticate with the host that is being communicated with
- Exchange the key with the host
- Host encrypts the data with the key
- Uses TCP port 995 and 465



[TLS Security 4: SSL/TLS Certificates | Acunetix](#)

HTTPS is HTTP with the TLS, which is Transport Layer Security. HTTPS is mainly used with online data transfers that require encryption to be applied. When making an online transaction, you need the data to be secured. To do this, you need to use HTTPS.

HTTPS uses an X.509 certificate and asymmetric cryptography, which is to two key things:

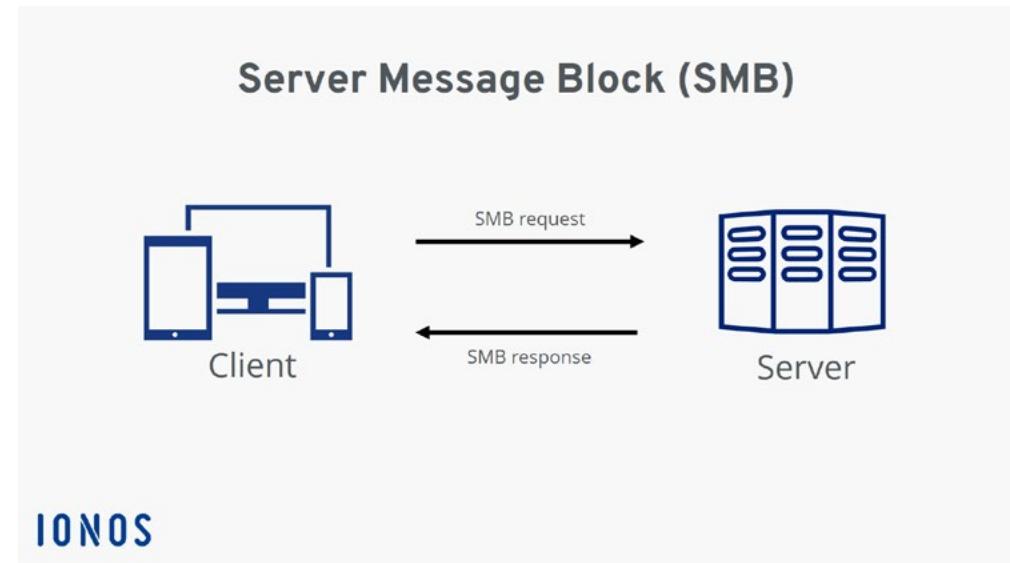
- authenticated with the host that is being communicated with
- Exchange the encryption key

The encryption key plays a key role with HTTPS because it is used to encrypt the information that will flow between two hosts. When the information is encrypted, it ensures its confidentiality and integrity.

HTTP with TLS uses TCP ports 995 and 465.

# Server Message Block (SMB)

- Is used for sharing access to printers and files over a Windows network
- Runs on various different ports:
  - TCP port 445
  - UDP port 137 and 138
  - TCP port 137 and 139 using NetBIOS



Windows use server Message Block, more commonly known as SMB, to share files and printers with various clients. With the help of SMB, a client on a Windows network can update, read, and write files on a remote server.

SMB uses different ports:

- TCP port 445
- UDP ports 137 and 138
- TCP port 137 and 139 using NetBIOS

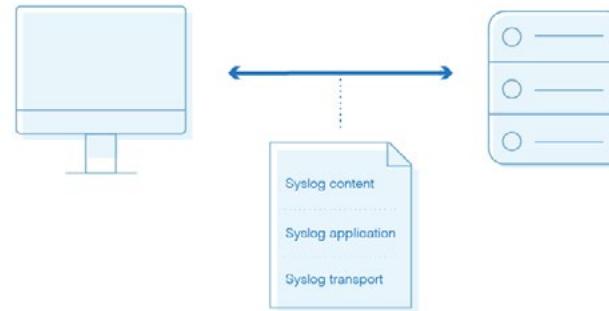


# Syslog

- Is used as a log repository that collects logs from various devices and servers on a network
- Allows you to sort and search logs
- Allows you to use various severity levels for events that are stored in logs
- Uses UDP port 514

## What Is Syslog?

The syslog protocol transports messages from network devices to a logging server

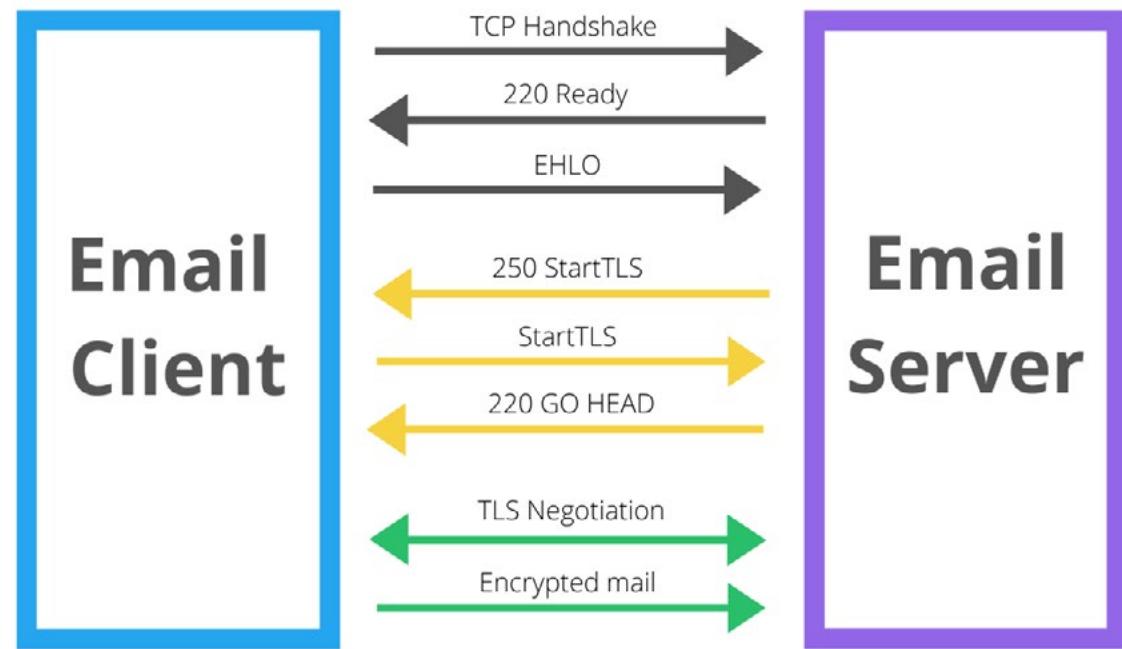


[What Is Syslog & Syslog Server? Guide & Recommended Tool - DNSstuff](#)

When you have several servers and network devices and want to collect events information from them into a centralized place, you can use syslog. All the configured devices and servers send their events information to the syslog server, allowing you to sort, review, search, and filter them. You can even assign severity levels to the events that have gathered. For example, an event that requires immediate attention is Severity 2. If the system is down, it is a Severity 0 event. A syslog uses UDP port 514.

# SMTP TLS

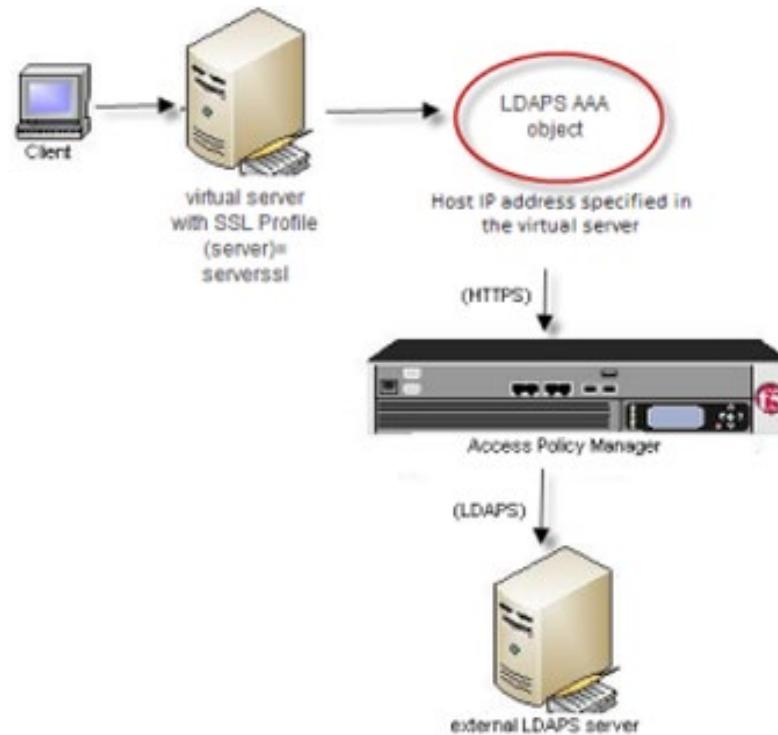
- Is SMTP with TLS for email encryption
- Uses TCP port 587



SMTP sends the emails in clear text, which obviously can be sniffed. However, when you use SMTP with TLS, the email is encrypted, safeguards the information stored within the email. Other than the encryption, the rest of the functionality remains the same as SMTP.  
SMTP TLS uses TCP port 587.

# Lightweight Directory Access Protocol (SSL) (LDAPS)

- Is LDAP protocol with SSL for securing the LDAP traffic
- Requires a certificate from a certification authority
- Uses TCP port 636



[AskF5 | Manual Chapter: LDAP and LDAPS Authentication](#)

LDAP exchanges information in cleartext. So, it is not easy to protect information that is in transit. To safeguard the information in transit, you can use LDAP with SSL to encrypt the information. To use SSL with LDAP, you need to have a certificate from a trusted certificate authority. LDAPS or LDAP with SSL uses TCP port 636.

# IMAP over SSL

- Is the IMAP protocol with SSL for email security
- Uses TCP port 993

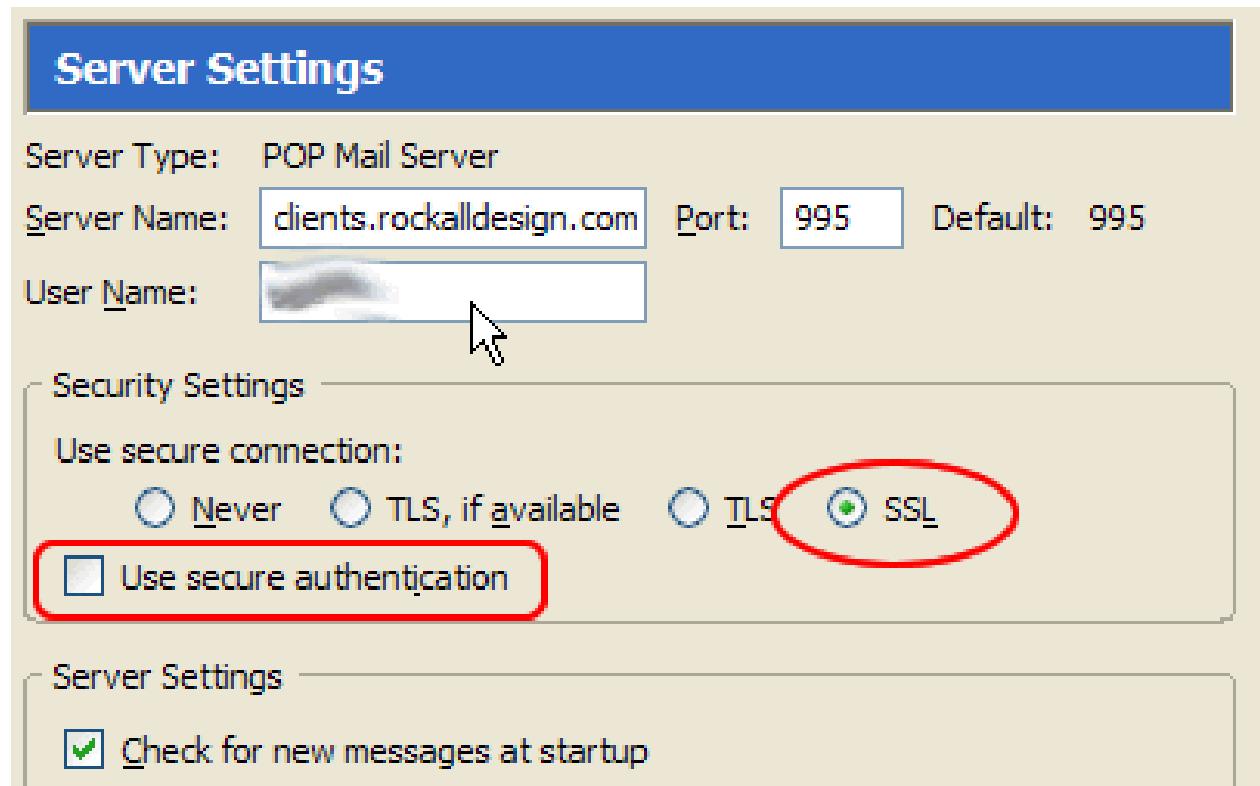


[Does ServWise provide Secure SMTP, POP3, IMAP \(SSL and TLS\)? - ServWise](#)

Similar to SMTP, IMAP can be configured with SSL, which provides encryption to the emails that are being downloaded.  
IMAP over SSL uses TCP port 993.

# POP3 over SSL

- Is the POP3 protocol with SSL that is used for encryption
- Uses TCP port 995



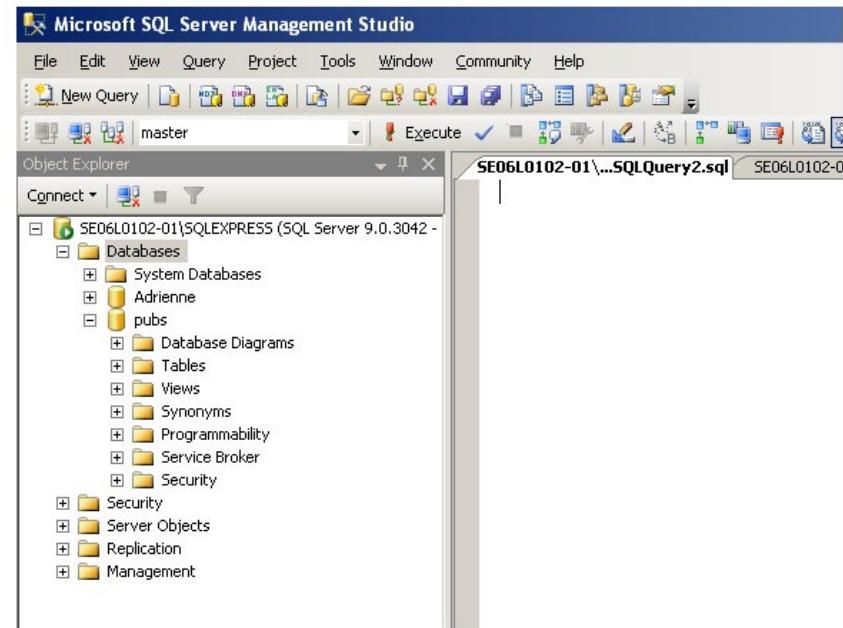
[POP3 + SSL = Secure Email ? | Wed 16 Sep 2009 | Blog | CodeStore](#)

POP3 also downloaded the emails in cleartext. You can use POP3 over SSL to safeguard the emails, which encrypts the information. The rest of the functionality remains the same as POP3.

POP3 uses TCP port 995.

# Structured Query Language (SQL) Server

- Is a Relational Database Management System (RDBMS) server
- Is used for data storage at the enterprise level
- Uses TCP port 1433

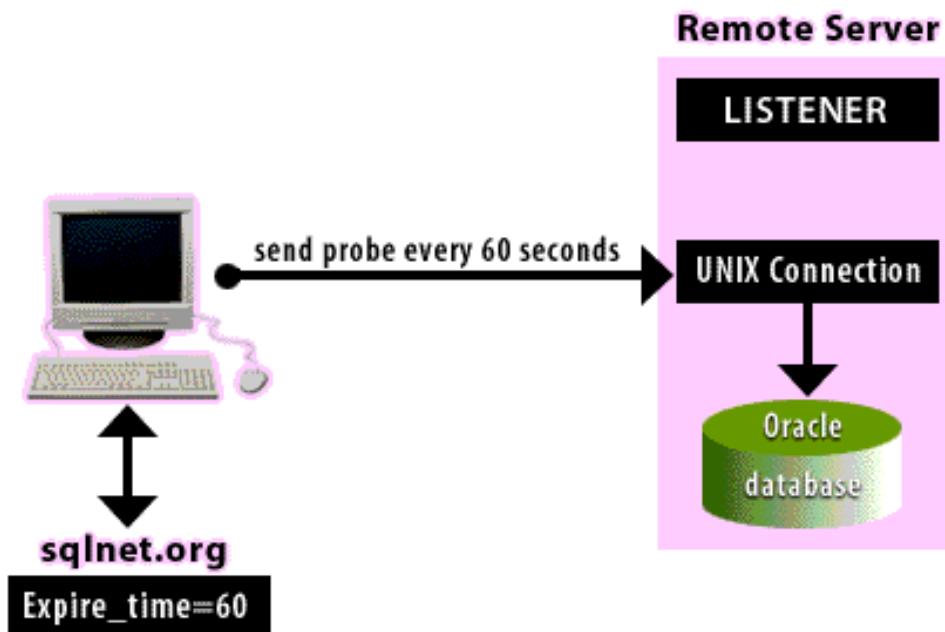


[Chapter 15 SQL Structured Query Language – Database Design – 2nd Edition \(opentextbc.ca\)](#)

Microsoft SQL Server is a relational database management system (RDBMS). It is used for storing a large amount of data and serves as a backend for enterprise applications. When configured with the applications, it allows you to update data stored as records. You can add, delete, modify, or search records. SQL Server uses TCP port 1433.

# SQLnet

- Is used for communication between a database server and clients
- Is used for allowing the applications to communicate with the databases running on different systems
- Uses TCP port 1521



[sqlnet.ora file \(characteristics\) \(relationaldbdesign.com\)](#)

SQLNet is used for communication between a database server and clients. When the server and clients are configured on different systems, you can use SQLNet to communicate with each other as if they are residing on the same system. SQLNet is not used because TCP/IP is the default protocol used on the networks. SQLNet uses TCP port 1521.

# MySQL

- Is a Relational Database Management System (RDBMS)
- Uses Structured Query Language (SQL)
- Is used as a backend for an application
- Uses TCP port 3306



[File:Database-mysql.svg - Wikimedia Commons](#)

Like Microsoft SQL Server, MySQL is another RDBMS used for data storage and management. MySQL comes in different variants and is also open-source and free. You can download the community edition and use it freely.

Like the SQL server, it is used as a backend for applications.  
MySQL uses TCP port 3306

# Remote Desktop Protocol (RDP)

- Is a remote connectivity protocol for Windows
- Provides the graphical user interface (GUI) when connected to the remote system
- Works with Windows and MAC
- Uses TCP port 3389



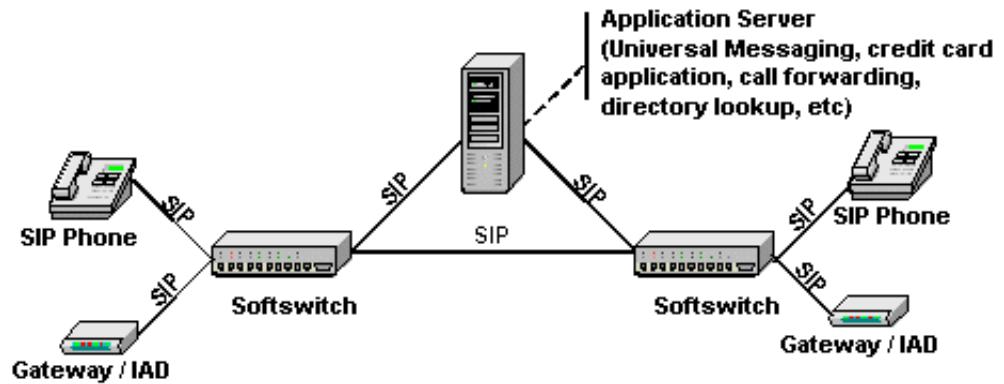
[Introduction to RDP - Remote Desktop Protocol \(heresjaken.com\)](http://heresjaken.com)

SSH is used for managing Linux and UNIX systems. Similarly, RDP or Remote Desktop Protocol is used with Windows systems. It is used for remotely connecting to Windows systems. Unlike SSH, which works on the command line, RDP uses a GUI interface. Initially, RDP was designed only for Windows, but now it is available on MAC systems.

RDP uses TCP port 3389.

# Session Initiation Protocol (SIP)

- Uses TCP or UDP port 5060/TCP port 5061
- Is used for:
  - Online games
  - Instant messaging
  - Streaming media
  - Videoconferencing
  - Audio and video calls



[What is Session Initiation Protocol \(SIP\)?](#)

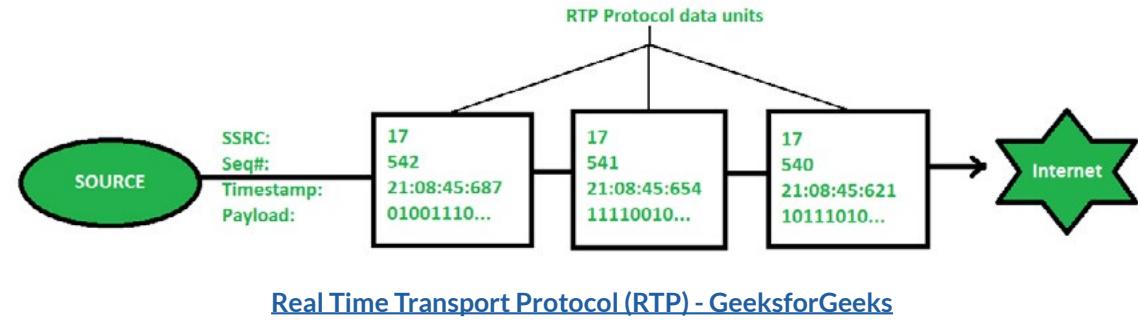
[\(\[metaswitch.com\]\(http://metaswitch.com\)\)](http://metaswitch.com)

Session Initiation Protocol or SIP is a signaling control protocol used with real-time communication. It initiates, manages, and terminates the real-time sessions. Think of a video call – this is where SIP is being used. Other uses cases are voice calls, such as VoIP, videoconferencing, and online games.

SIP uses TCP or UDP port 5060. It also uses TCP 5061.

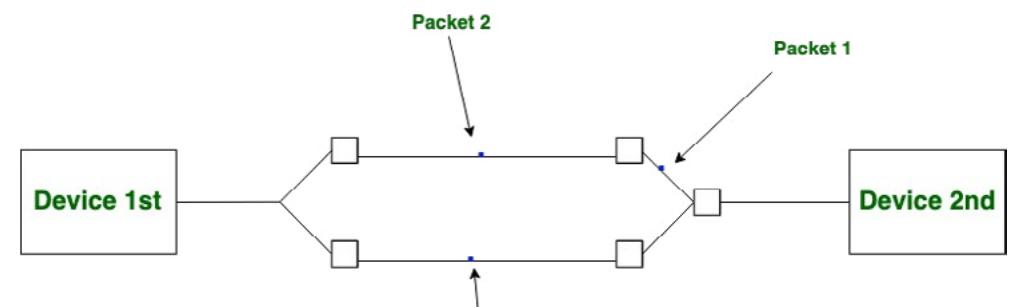
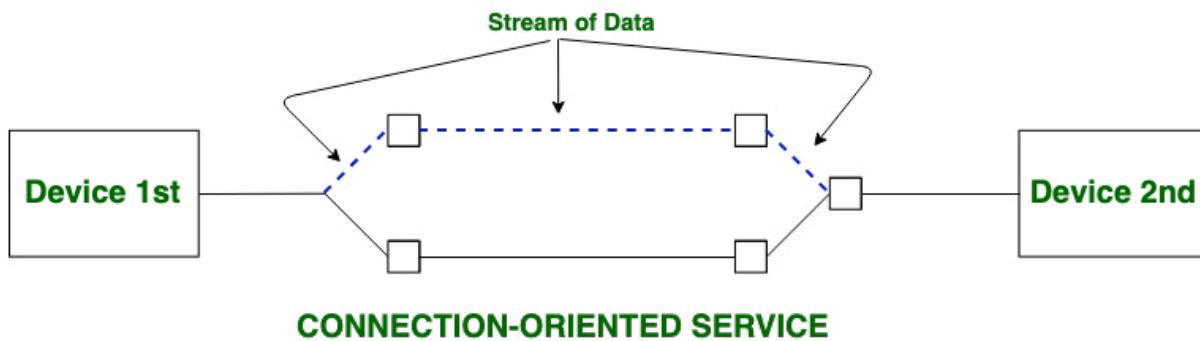
# Real-time Transport Protocol (RTP)

- Is a multicast protocol
- Is designed for audio and video delivery over the Internet
- Is now a standard for Voice over IP (VoIP)
- Uses UDP port 5004/TCP port 5005



RTP or Real-time Transport Protocol is a multicast protocol, but it can be used with unicast applications. It is designed to be used with the audio and video delivered over the Internet. Like SIP, RTP is also used with voice over IP (VoIP). However, the fundamental difference between SIP and RTP is that RTP is a payload protocol that sends and receives audio over the Internet. It can also be used with streaming media and video conferencing.

# Connectionless vs. Connection-oriented



[Difference between Connection-oriented and Connection-less Services - GeeksforGeeks](#)

## CONNECTIONLESS SERVICE

When packets travel over a network, they can be sent using either connection-oriented or connection-less methods depending on the type of application and protocols used. A connection needs to be formed first for the packets to travel from a source to the destination system or device.

So, there are two types of connection-related services. The first is the connection-oriented service, which creates a connection between the sender and receiver. A connection is established. When the work is done, the connection is terminated. All packets traveling to the destination follow one path and the sequence they were sent in. This ensures the reliability of packet delivery.

In contrast, connection-less service does not include ensuring service delivery, which means that there is no reliability whether the packets will be delivered or not. The packets take a different path to reach the destination, which means they may or may not reach the destination in the sequence.

# Summary



## Protocols



That's the end of the lesson.  
Here we covered :

- Protocols



A photograph of a person's hands holding a silver smartphone. Floating around the phone are several light gray circular icons representing communication and networking, such as people, messages, and email symbols. The background is a dark purple.

*NEXT TOPIC*

# NETWORK SERVICES

Lesson

# 6

# Network Services

- 1 — Welcome to the lesson 6 of Module 1. In this lesson, you will learn about the:
- 2 — Various networking protocols and their ports.



Network Fundamentals

# Agenda

- DHCP
- DNS
- NTP



Hi, welcome to COMPTIA Network+ Course  
In this lesson, we will talk about:

- DHCP
- DNS
- NTP





*TOPIC 1*

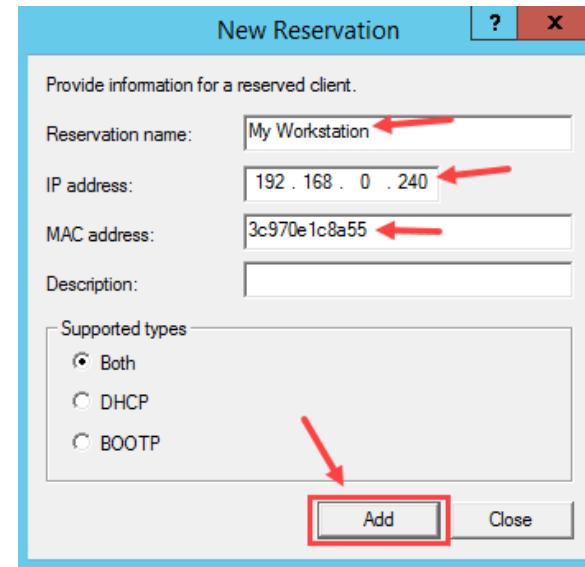
---

# DHCP

---

# Scope, Exclusion Range, and Reservation

- DHCP Scope
  - Is a range of consecutive IP addresses that are leased to the clients
- Exclusion Range
  - Is a range of IP addresses that are defined within a DHCP scope
  - Are excluded from being leased to the clients
- Reservation
  - Is used to assign the same IP address to the client
  - Is tied to the client's MAC address
  - Prevents the same IP address to be assigned to other hosts



[Configure DHCP Reservation in Windows Server 2012 R2 \(mustbegeek.com\)](#)

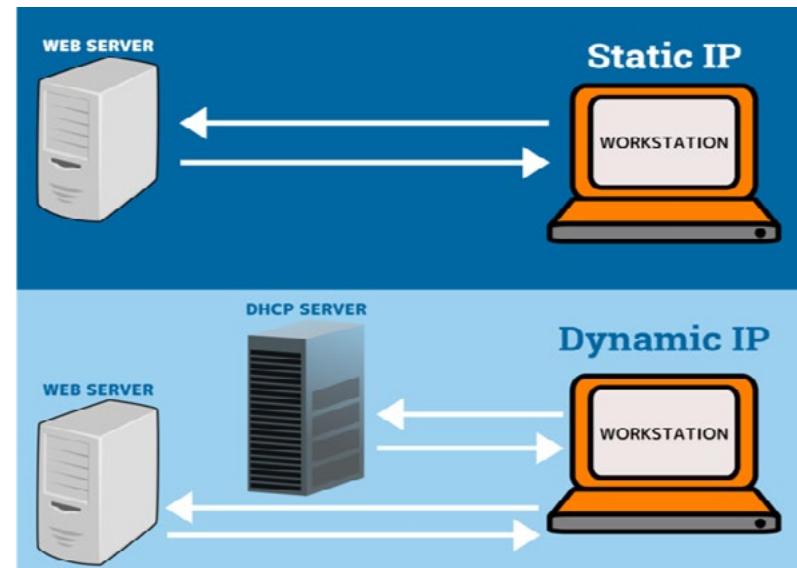
A DHCP server is used for leasing the IP addresses to the network clients. The DHCP server does not start releasing the IP addresses ad hoc. It has to have a defined pool of IP addresses that it can lease. The IP address pool is the DHCP scope, which is the range of consecutive IP addresses leased to the clients. For example, a DHCP scope has a range of IP addresses: 10.10.10.1 to 10.10.10.254. This is a consecutive range. When clients connect to the network, the IP addresses are released to them until the pool is exhausted.

There may be certain IP addresses from a given pool that you do not want to lease out to the clients. You can exclude these IP addresses from the DHCP scope. When you exclude these IP addresses, they are not leaseable to the clients.

You may also have network devices or servers that need to have fixed IP addresses. For example, a Web server cannot have a dynamic IP address. It needs to have a fixed IP address. To assign it a fixed IP address, you can reserve the IP address for the Web server by binding it with its MAC address. DHCP knows that it is a reserved IP address and does not lease it to the other clients when this is done. The Web server will always get the same IP address.

# Dynamic and Static Assignment

- Dynamic
  - Is assigned using DHCP
  - Is used when there are a large number of clients
- Static
  - Is manually assigned to the clients
  - Is assigned on the servers
  - Is used when there are a small number of systems



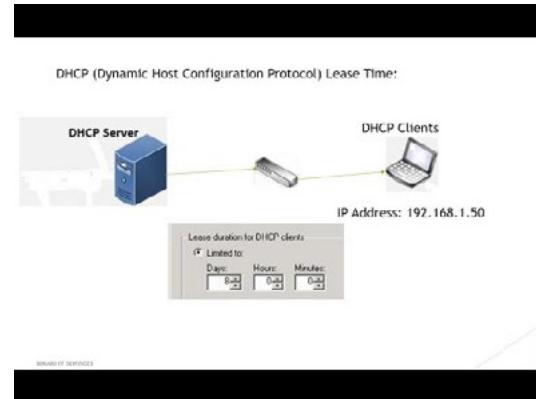
[Static IP vs. Dynamic IP | Make the Right Choice Today! | Netpluz Asia](#)

To be part of a network, a device or a system needs an IP address, which can either be fixed or dynamically assigned by a DHCP server. A dynamic IP address is assigned when there are many systems on a network. It is not possible for the network administrator to manually assign fixed IP addresses to the systems. The solution is to use a DHCP server to manage the IP address allocation without any manual intervention.

The static IP address is manually assigned to the clients. You have server and network devices, such as routers that cannot have dynamic IP addresses. They need to have a fixed or static IP address, which must be manually assigned. Also, when you have a limited number of systems, such as 6 or 7 or maybe 10, you can assign static IP addresses to them.

# Lease Time and Available Leases

- Lease Time
  - Is the time that the clients are assigned an IP address
  - Is for a specific time – such as eight hours
- Available Leases
  - Is the number of leases available in a scope

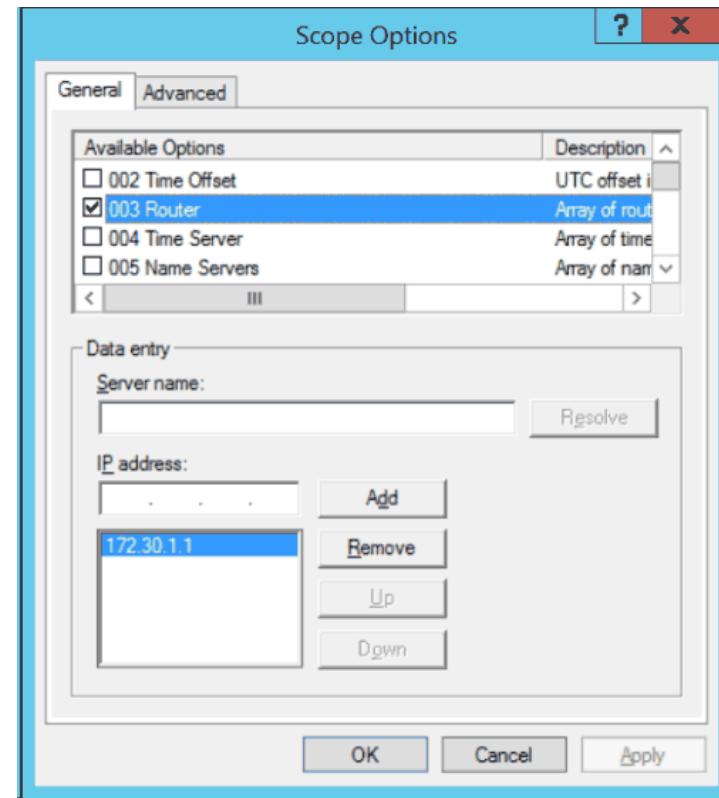


[What is DHCP Lease Time - YouTube](#)

The lease time is when a client is allocated an IP address. For example, a DHCP server has been configured to lease the IP addresses for 8 days or 8 hours. It depends on the configuration, but there is no hard and fast rule. When an IP address is assigned to a system, it is assigned in the DHCP pool and is not assigned to another system. When a DHCP starts leasing the IP addresses, only a specific set of IP addresses are left from its scope. These are known as the available leases.

# Scope Options

- Is a set of additional information that is assigned to the client by a DHCP server with an IP address
  - 003 Router List: List of IP addresses as the default gateway
  - 005 Name Servers: List of available DNS servers.
  - 015 DNS Domain Name: The fully-qualified domain name suffix for a client
  - 042 NTP Servers: List of NTP servers

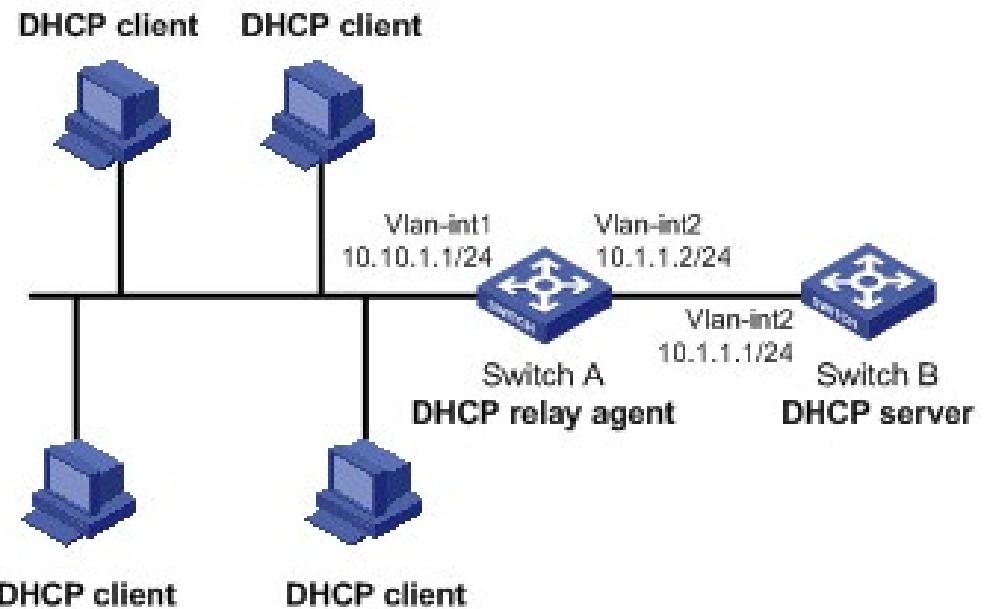


[Step-by-Step Creating a Windows Server DHCP Scope - Serverlab](#)

When an IP address is assigned to a system on a network through DHCP, a few more parameters are assigned as well. Along with the IP address, parameters like DNS server, gateway, and subnet mask are also assigned. These parameters need to be configured in the scope options in DHCP. For example, you may want to assign 192.168.10.1 as the DNS server to all clients that obtain dynamic IP addresses. You need to configure the DNS or Name server parameter in the scope in such a case. Some of the critical parameters are displayed on the slide.

# DHCP Relay

- Forwards the DHCP packets between the client and DHCP server
- Is required when a client and DHCP server is not on the same network
  - If not configured, router will discard the broadcast packet sent by the client



[DHCP relay agent configuration example \(hpe.com\)](#)

You may have a single DHCP server that needs to lease IP addresses to the different VLANs on an extensive network. To provide IP addresses to the systems on different VLANs, you need to configure the DHCP relay on routers configured on each VLAN. By default, the routers discard the broadcast messages. On the other hand, a DHCP client sends a broadcast message to the DHCP server to obtain an IP address. When a router receives a broadcast message, it will simply discard it. You may have to put a DHCP server on each VLAN to handle this situation, which may not be a possible solution. However, as an alternate solution, you can configure the DHCP relay agent on the routers responsible for forwarding the broadcast messages to the DHCP server as a unicast message. The DHCP server knows that a client only sends a broadcast message. It checks the gateway address in the unicast message and locates the scope with the same gateway address. Once the scope is located, it sends back a unicast message with an IP address and reverts to the DHCP relay. The DHCP relay agent then converts the unicast message to the broadcast message and forwards it to the client that requested the IP address.

# IP Helper/UDP Forwarding

- Forwards the DHCP packets between clients and servers
- Is found in Windows to keep the system updated with the network modifications

IP Helper is responsible for forwarding the DHCP packets between the DHCP server and its clients. It is found in the Windows systems to keep the system updated with the network modifications.



## *TOPIC 2*

---

# DNS

---

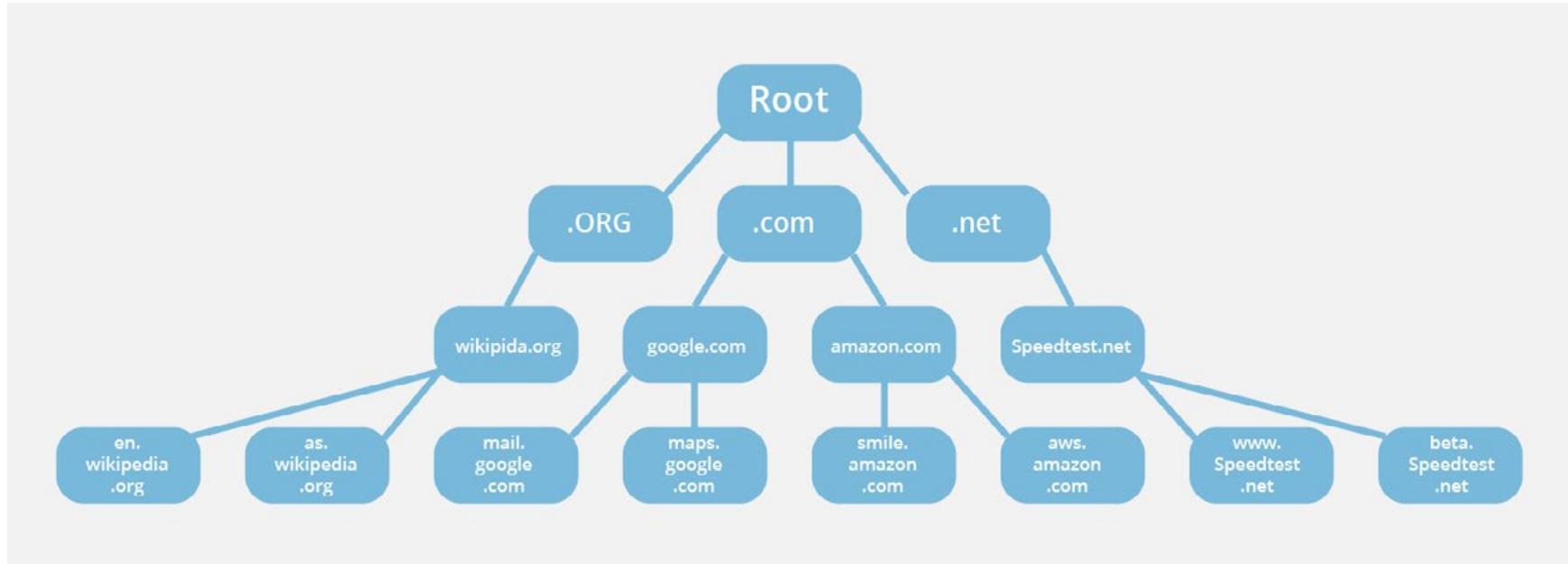
# Record Types

DNS Record	Description
A	Provides the IP address of the specified domain
AAAA	Maps the hostname to an IPv6 address
Canonical name (CNAME)	Is an alias name for a domain
Mail exchange (MX)	Is used for defining the message routing
Start of authority (SOA)	Provides the administrative information for a domain. Administrative information can include name of the administrator, domain updation time, refresh time, and time-to-live.
Pointer (PTR)	Is used for reverse DNS lookup, IP address to domain name lookup
Text (TXT)	TXT (SPF) - specifies a list of authorized hostnames or IP addresses from which a mail can trigger in a domain TXT (DKIM) Domain Keys Identified Mail - provides authentication of mail sent and received by the same messaging server.
Service (SRV)	Is a service location record that specifies a port number in addition to the IP address.
Name server (NS)	Defines the domain name for the DNS server

A DNS server is responsible for name resolution. To do this, the DNS server works with various types of records that perform different types of name resolution tasks. The essential DNS records are:

- A: Provides the IP address of the specified domain
- AAAA: Maps the hostname to an IPv6 address
- Canonical name (CNAME): Is an alias name for a domain
- Mail exchange (MX): This is used for defining the message routing
- Start of Authority (SOA): Provides the administrative information. Administrative information can include the name of the administrator, domain updation time, refresh time, and time-to-live.
- Pointer (PTR): Is used for reverse DNS lookup, IP address to domain name lookup
- Text (TXT): Works with two different records:
  - TXT (SPF) - specifies a list of authorized host names or IP addresses from which a mail can trigger in a domain
  - TXT (DKIM): Is Domain Keys Identified Mail. It provides authentication of mail sent and received by the same messaging server.
- Service (SRV): Is a service location record that specifies a port number in addition to the IP address.
- Name server (NS): Defines the domain name for the DNS server

# Global Hierarchy – Root Servers



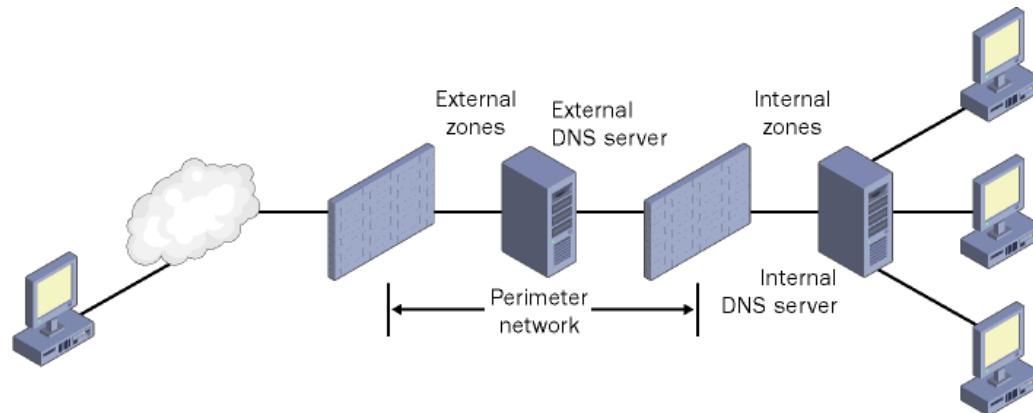
[DNS root server | Cloudflare](#)

DNS follows a tree-like hierarchy. The top is the root zone, which is responsible for answering the queries for the records that they have stored. The DNS servers in the root zone can also query based on the cache they have stored.

Below the root zone, a Top Level Domain (TLD) server receives queries from the DNS servers in the root zone. Below the TLD servers are the DNS servers that hold the domain names.

# Internal vs. External

- External
- Used as authoritative-only to handle public queries
- Internal
- Is used for internal purposes
- Can contain authoritative information from the external DNS servers



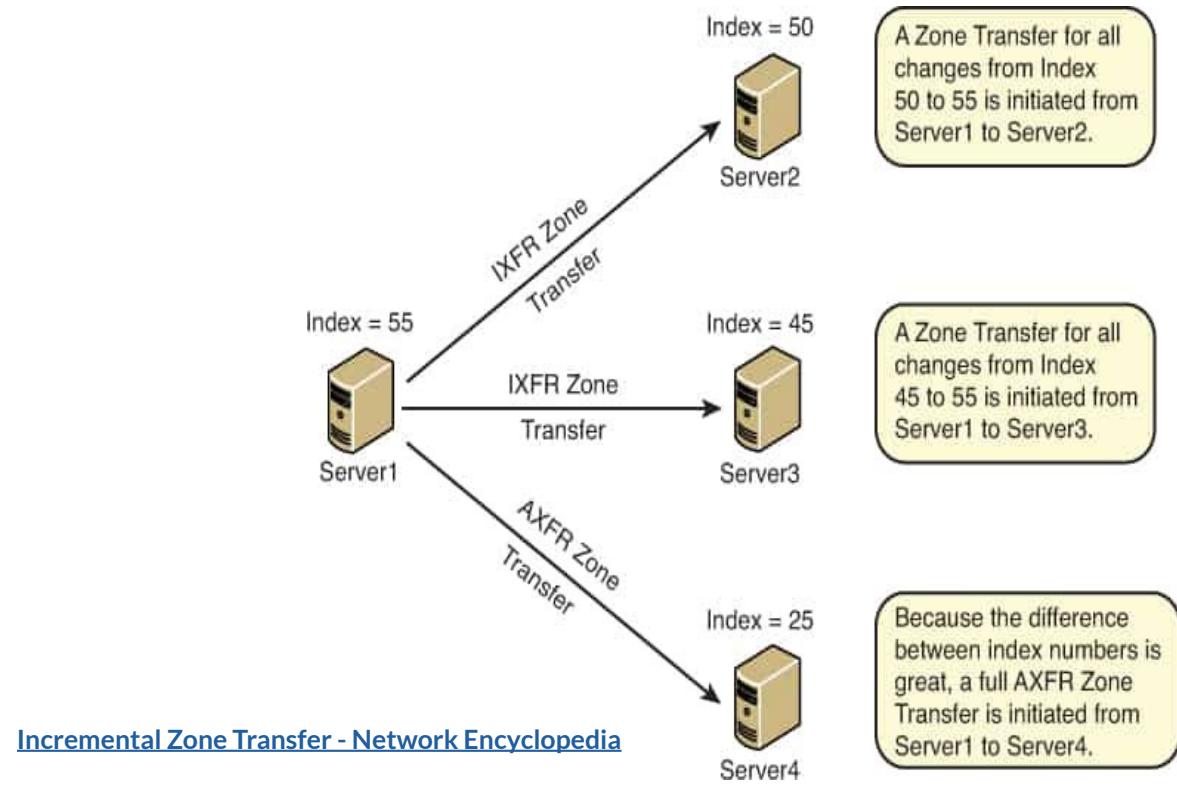
[Securing DNS Servers | Microsoft Windows Security Resource Kit \(flylib.com\)](#)

DNS servers can either be internal or external to an organization. The external DNS servers are mainly configured to answer public queries. They are authoritative. For example, if an external DNS server is authoritative for [www.microsoft.com](http://www.microsoft.com), it will handle these queries.

The internal DNS servers are responsible for the name resolution for the internal services and hosts. However, they can contain authoritative information from the external DNS server even though both should be kept separate from the security point of view. The internal and external DNS servers should not know each other.

# Zone Transfers

- Replicating the zone to the secondary DNS server:
- Redundancy
- Load balancing
- Can be incremental or full depending on the changes required to be replicated



An organization may have more than one DNS server. If they do, these DNS servers need to be in synchronization so that if the primary DNS server, with all the zone information, goes down, the secondary DNS server can serve the clients. Another reason for having more than one DNS server is distributing the DNS queries workload across multiple DNS servers.

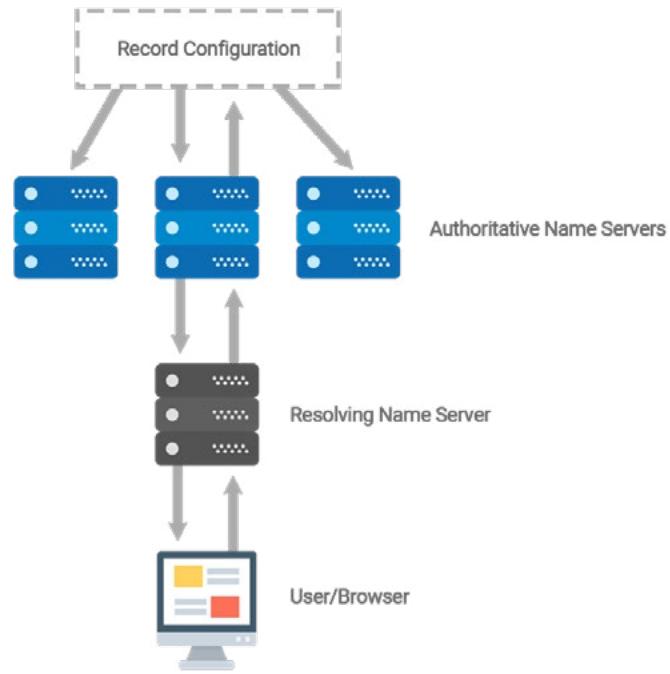
The core intent of the zone transfer is to replicate the zone file from one server to another server. When you have a single DNS server and configure another DNS server, the zone server starts between both servers. After the initial replication, depending on the number of changes in the primary server, the zone transfer can be incremental or full.

Another reason for zone transfer is the refresh interval defined in the state of authority (SOA) record. When the refresh interval expires, the zone transfer is initiated. One of the core reasons for zone transfer is when changes are made to the zone file on the primary DNS server. If there are changes, the secondary DNS server is notified of the zone changes. The secondary DNS server then initiates the changes immediately.

It is important to note that the primary DNS server never initiates the zone transfer. The secondary DNS server always owns the responsibility of zone transfer from the primary DNS server.

# Authoritative Name Servers

- Hold the authority for a zone
- Are queried by the recursive name servers for DNS records



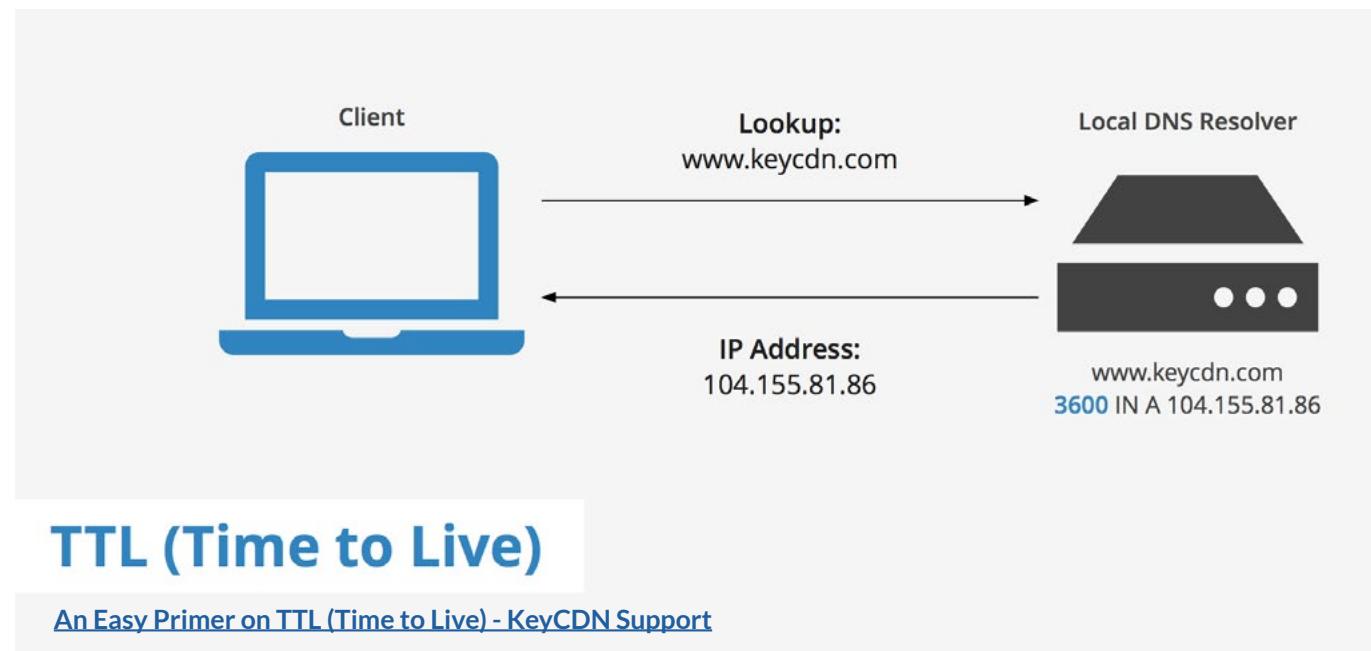
[Authoritative vs. Recursive DNS Servers:  
What's The Difference? \(dnsmadeeasy.com\)](http://dnsmadeeasy.com)

An authoritative DNS server holds the authority for a particular zone. The other DNS servers send the queries to the authoritative DNS servers for name resolution. It is important to note that the authoritative DNS servers are NEVER authoritative for the data it caches. It is authoritative only for the information that it holds.

Let's take an example. You launch your Web browser and enter [www.microsoft.com](http://www.microsoft.com) as the website name you want to visit. Your organization's DNS server does not store this information and does not contain this information in the cache either. In this case, your DNS server is acting like a recursive DNS server that will forward the request to the correct DNS server that is authoritative. Once it gets the information back, it responds to the web browser with the correct information.

# Time To Live (TTL)

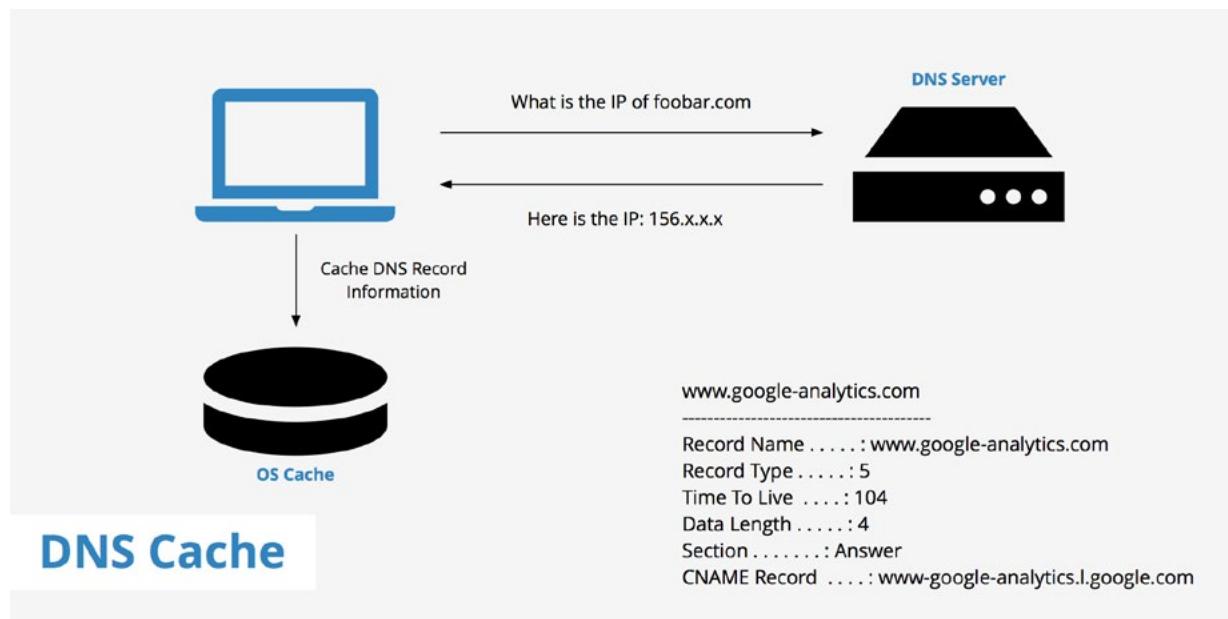
- Is a field in the DNS reply
- Defines the duration for which the client should store the reply



Each DNS query has a specific lifetime. When you send a query to a DNS server, it replies with an answer. The reply contains a time to live or TTL field that defines the lifetime duration of the query that will be cached at the client end. Let's say that you browse for [www.microsoft.com](http://www.microsoft.com). The website loads in your Web browser. This query is now stored in the DNS cache on your system. Within its TTL period, if you again browse for [www.microsoft.com](http://www.microsoft.com), the request is first checked against the DNS cache record. If the request is mapped, then the domain name is resolved locally. However, if TTL has expired, the query is no longer stored in the cache.

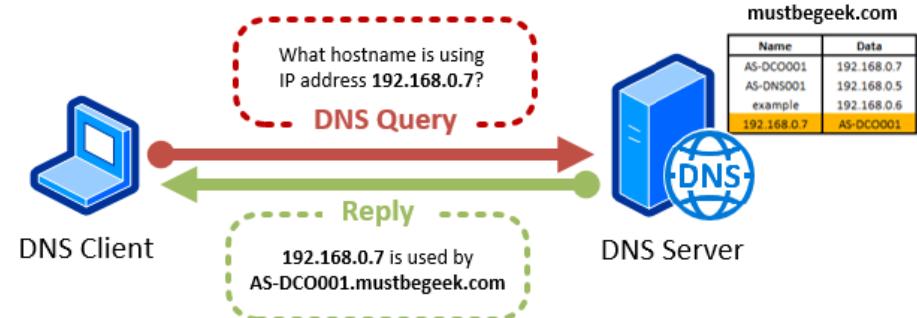
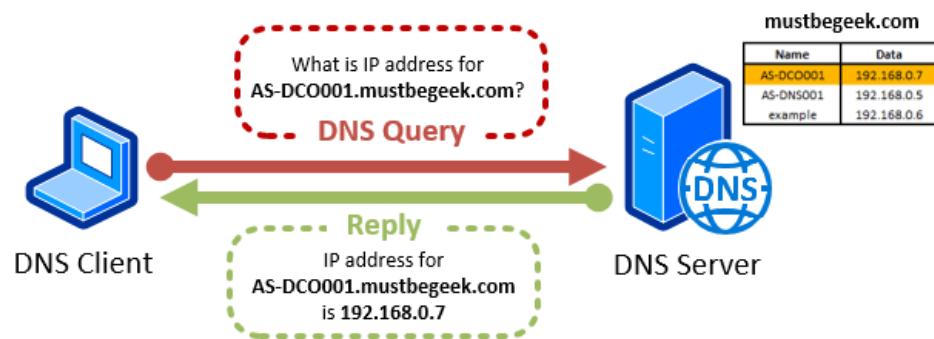
# DNS Caching

- Is a temporary storage that contains the old DNS lookups
  - Can be by a Web browser
  - Can be by an operating system



As discussed in the previous slide, the DNS cache stored the DNS queries for a specific time. When the queries are stored locally in the cache, the name resolution occurs locally on the system. The DNS cache is the first place where the DNS queries search for an answer. So, in a nutshell, DNS cache works like temporary storage for the DNS requests. If you visit a website for the first time, it is stored in the DNS cache. The subsequent request to the same website is checked against the DNS cache. The entries in the DNS cache can be made by a Web browser or the operating system.

# Reverse DNS/Reverse Lookup/Forward Lookup

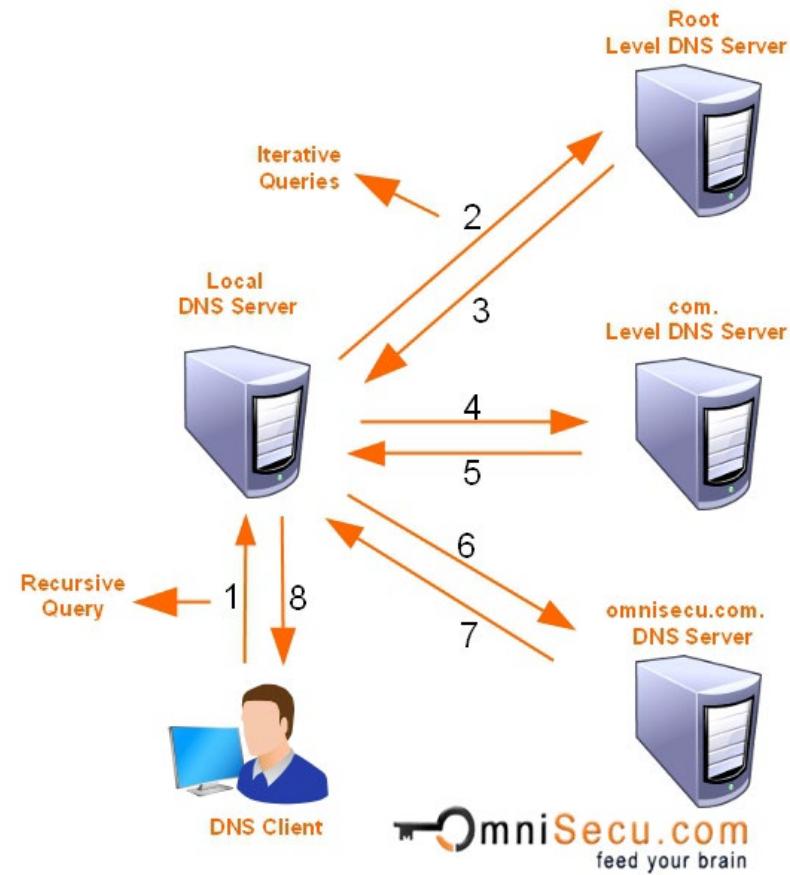


[Understanding Forward and Reverse Lookup Zones in DNS \(mustbegeek.com\)](#)

A DNS server can hold the forward and reverse lookup zones. The forward lookup zone is used to resolve the hostname to the IP address. The reverse lookup zone performs the reverse operations, IP address to the hostname.

# Recursive Lookup/Iterative Lookup

- Recursive Query:
  - DNS client queries the DNS server
  - DNS server responds with an answer or can query other DNS servers
- Iterative Query:
  - DNS client queries the DNS server
  - DNS server responds with an answer
  - If not, it queries the highest-level DNS server and is referred to the authoritative DNS server



[Recursive and Iterative DNS Queries \(omnisecu.com\)](#)

A query sent to a DNS server can be of two types. The first one is the recursive query. It works in the following manner:

- DNS client queries the DNS server
- DNS server responds with an answer or can query other DNS servers

On the other hand, the iterative query works in the following manner:

- DNS client queries the DNS server
- DNS server responds with an answer
- If not, it queries the highest-level DNS server and is referred to the authoritative DNS server

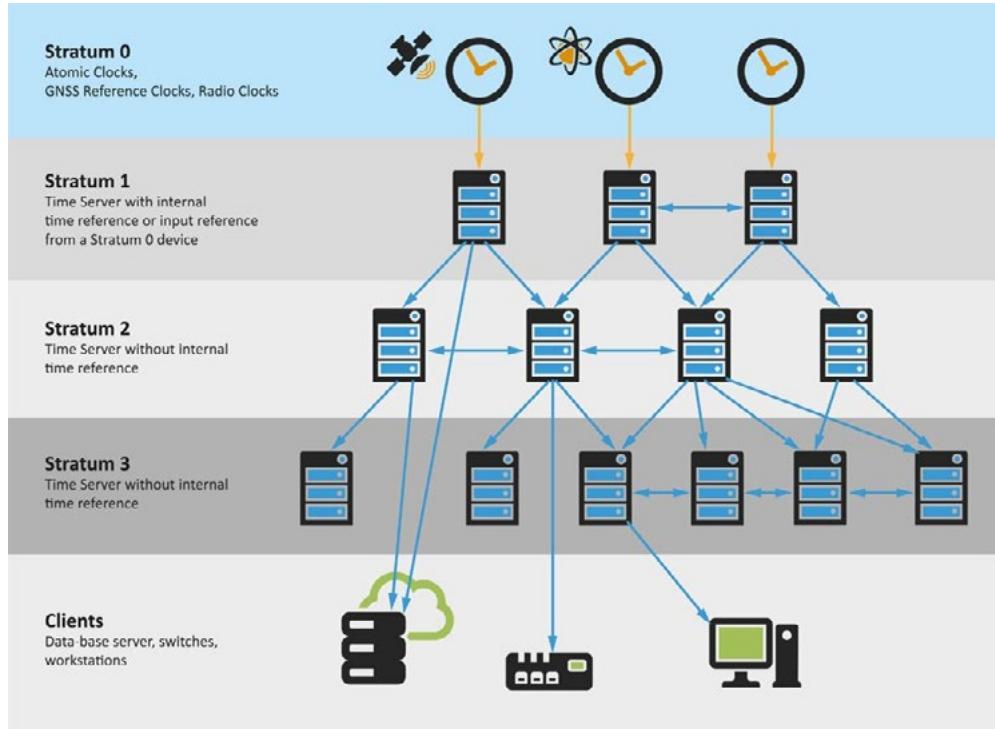
# *TOPIC 3*

## DNS



# Stratum

- Indicates the accurate time source
- Is a hierarchy of stratum levels
- Lower the number, more accurate time is
- Starts with 0 to 15
- Level 16 indicates that the device is unsynchronized

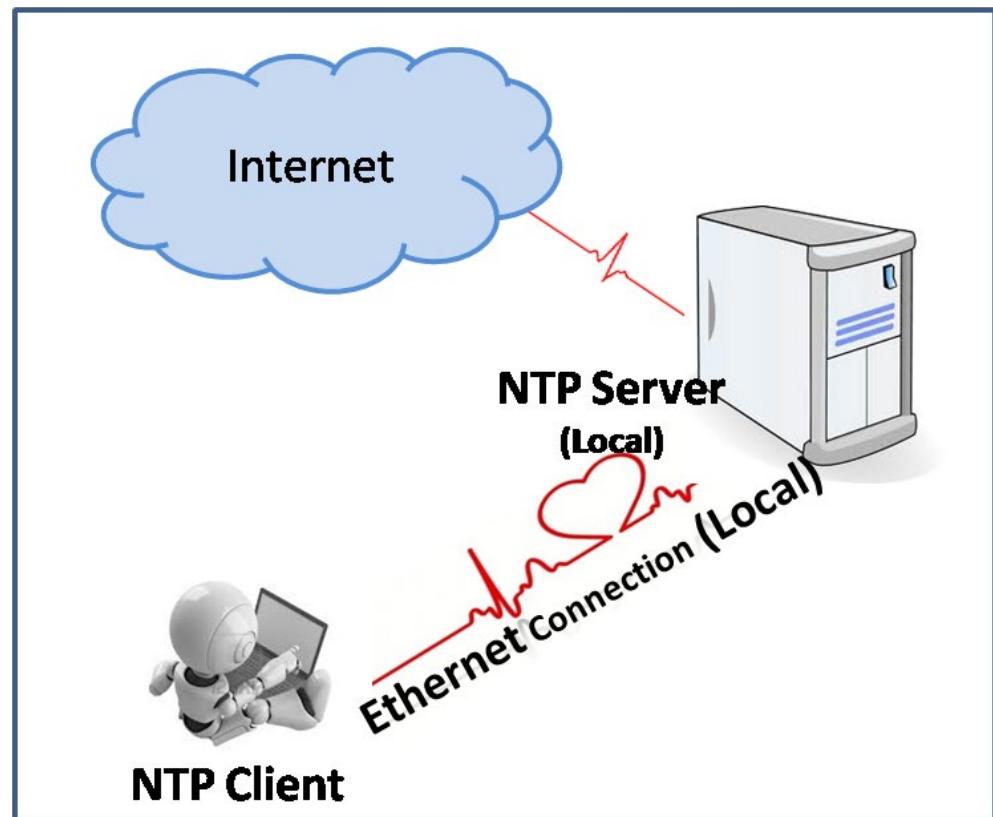


[Joining the NTP Pool \(parkercs.tech\)](http://parkercs.tech)

The stratum level defines the time accuracy. It starts with 0 and goes up to level 15. The higher the stratum level, the lower the time accuracy is. For example, stratum level 0, the atomic clocks, provides the most accurate time. There will be slightly less accuracy at level 1, which goes for level 2. Level 15th is the last level that can be synchronized with the lower level. If a device indicates level 16, it simply means unsynchronized with the NTP server.

# Clients

- Query the NTP servers using the NTP protocol



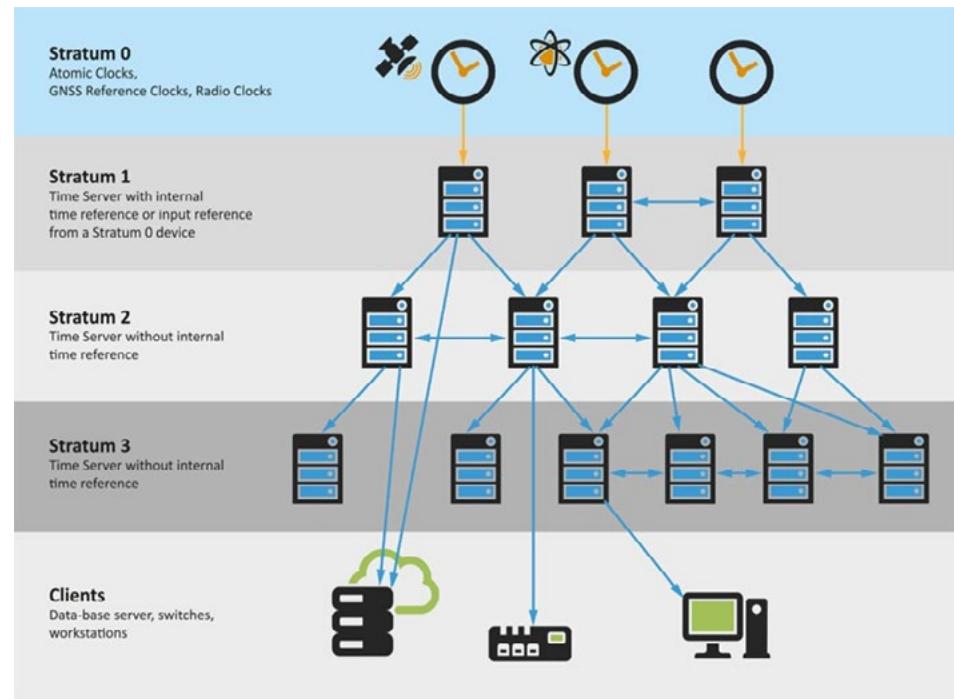
[Set up NTP Server on Linux Server | Wadhah DAOUEHI](#)

An NTP client is software that connects with the NTP server for time synchronization. The majority of the network devices have a built-in NTP client. For example, you have an NTP client in a router or a switch, and that is how they can synchronize their time with the NTP server. Even an operating system, such as Windows, has an NTP client.

NTP clients use the NTP protocol for time synchronization. They query the NTP server to keep their time-synchronized.

# Servers

- Are used to either synchronize time at the lower stratum levels or with the network devices
- Can be a specialized piece of hardware
- Are used by the networking device to synchronize clocks
- Synchronize with the atomic clocks
- Can be internal or external to a network



[Joining the NTP Pool \(parkercs.tech\)](#)

NTP servers can either synchronize with the lower stratum levels or with the network devices. Let's take the first one as the case point. It will be stratum level 2. If you have an NTP server at stratum level 4, it must synchronize with the lower level. THE NETWORK DEVICES MOST LIKELY USE the NTP server at stratum level 3 for time synchronization.

An NTP server can be configured on an operating system like Windows Server or even specialized hardware that synchronizes to the lower level. The lowest level is level 0, which is the atomic clock. The lower the stratum level, the more accurate time it has. Therefore, the lowest level, level 0, provides the most accurate time.

NTP servers can be configured as an internal server or external. If you need to synchronize your internal NTP servers, you can find the NTP servers available on the Internet. For example, [pool.ntp.org/zone/us](http://pool.ntp.org/zone/us) provides a list of NTP servers in the United States.

# Summary

- DHCP
- DNS
- NTP



That's the end of the lesson.  
Here we covered:

- DHCP
- DNS
- NTP





*NEXT TOPIC*

---

# CORPORATE AND DATACENTER NETWORK ARCHITECTURE

---

Lesson

7

# Corporate and Datacenter **Network Architecture**

- 1 — Welcome to the lesson 7 of Module 1. In this lesson, you will learn about the:
- 2 — Corporate and data center network architecture.



Network Fundamentals

# Agenda

- Three-tiered
- Software-defined Networking
- Spine and Leaf
- Traffic Flows
- Branch Office vs. On-premises Datacenter vs. Colocation
- Storage Area Networks



Hi, welcome to COMPTIA Network+ Course  
In this lesson, we will talk about:

- Three-tiered
- Software-defined Networking
- Spine and Leaf
- Traffic Flows
- Branch Office vs. On-premises Datacenter vs. Colocation
- Storage Area Networks



A photograph of four diverse business professionals laughing together in an office environment. A woman with curly hair and glasses is on the left, a man with glasses is in the center, another man is partially visible on the right, and a woman with blonde hair is on the far right. They are all dressed in professional attire. The background shows office equipment like a printer and a computer monitor.

# *TOPIC 1*

---

# THREE-TIERED

---

# Core

Access/Edge

Distribution/  
Aggregation

Core

- Is responsible for routing the traffic
  - Into the network
  - Out of the network
- Is made up of routers that perform the routing
- Can also have switches depending on the network architecture
  - Perform fast switching
- Contains high-speed devices with full hardware redundancy

Three-tier network architecture is commonly used when you have a large amount of ingress and egress traffic. Each tier plays a significant role in handling the traffic. The first tier is the core tier, which is responsible for ingress and egress traffic from a network. There are routers in this tier that route the traffic in and out of the network. With the help of routers, you can connect two or more different networks.

The core tier is designed with high-end switches to perform fast switching. The core tier can also contain the switches to perform switching of packets. The devices in the core tier are installed with the full hardware redundancy.



# Distribution/Aggregation

Access/Edge

Distribution/  
Aggregation

Core

- Is the second tier
- Is responsible for filtering the traffic
  - Uses access control lists
- Is the tier where network policies are defined
- Can contain Layer 3 switches and firewall
- Has hardware and network redundancy
- Connect with the access switches using high-speed uplinks

The second tier in the three-tiered network is the distribution or the aggregation tier. It uses access control lists to filter the traffic. You can also define network policies on this tier. You also have Layer 3 switches that are responsible to route packets within a network, which can have several subnets. You also implement various network devices, such as firewall, on this tier.

One of the key role of the aggregation or the distribution layer is to provide redundant interconnections with the switches that can also perform the layer 3 routing. The switches at this tier are configured with redundant connections, and redundant hardware, such as power and fans. The switches themselves are configured with the redundancy. The switches at this tier connect to the access switches, which connect the end clients, using high-speed uplinks. If one switch fails, the redundant switch carries the traffic to avoid any downtime.



# Access/Edge

## Access/Edge

## Distribution/ Aggregation

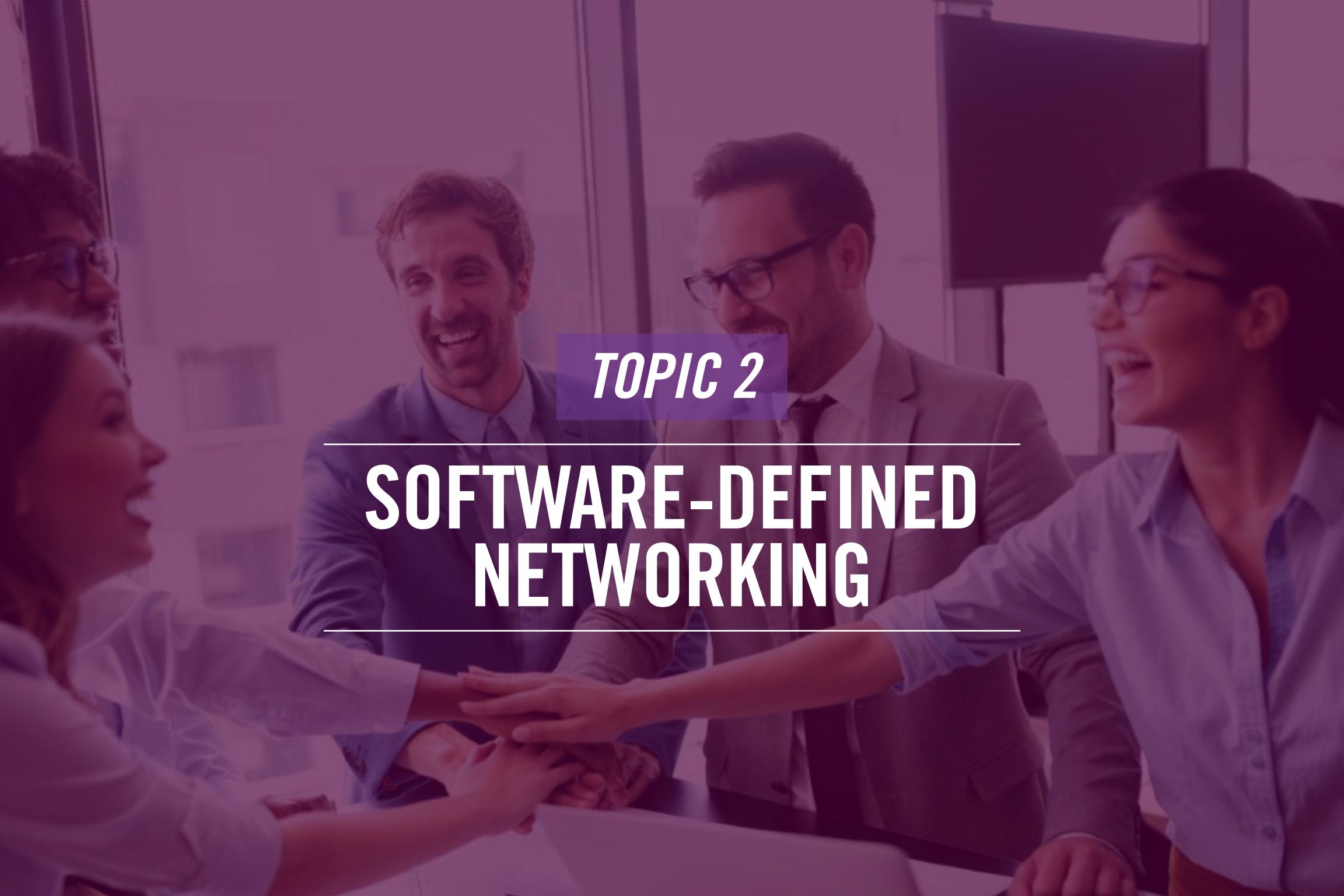
## Core

- Contains access switches that
  - Connect client systems
  - Connect servers
- Is responsible for segregating the traffic to be sent to appropriate VLAN
- Allows users to access network services

The third tier is the access or the edge tier. The access or the edge tier receives the packets from the distribution tier, and then it further segregates the traffic to the appropriate segments on the network. You have the switches that connect with the end clients on a network. The end clients can be the servers, systems, or any other client that exists on a network.

Most of the data is routed within the network at this tier, which also allows the users to access the network services. Since the data is restricted between the network, it is low-latency transmission between the servers or the network devices.



A group of diverse business people in a meeting, smiling and holding hands in a huddle.

*TOPIC 2*

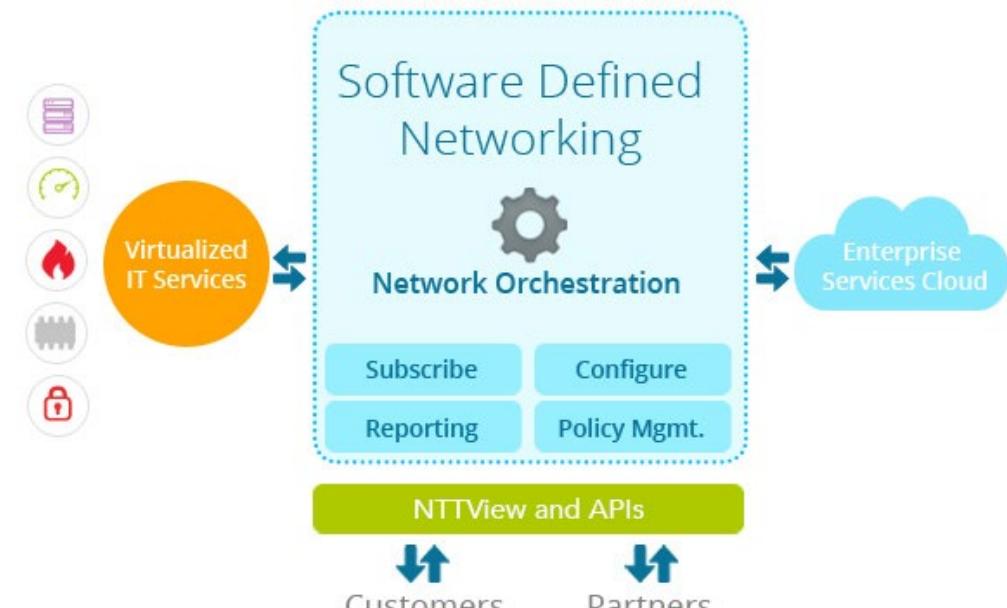
---

## SOFTWARE-DEFINED NETWORKING

---

# Software-defined Network

- Implements abstraction through different layers in a network
- Allows you to control the network without worrying about the underlying technologies
- Works in the vendor-neutral model
  - Integrate technologies from any vendor
  - Removes the complexity in a large network
  - Does not use proprietary protocols

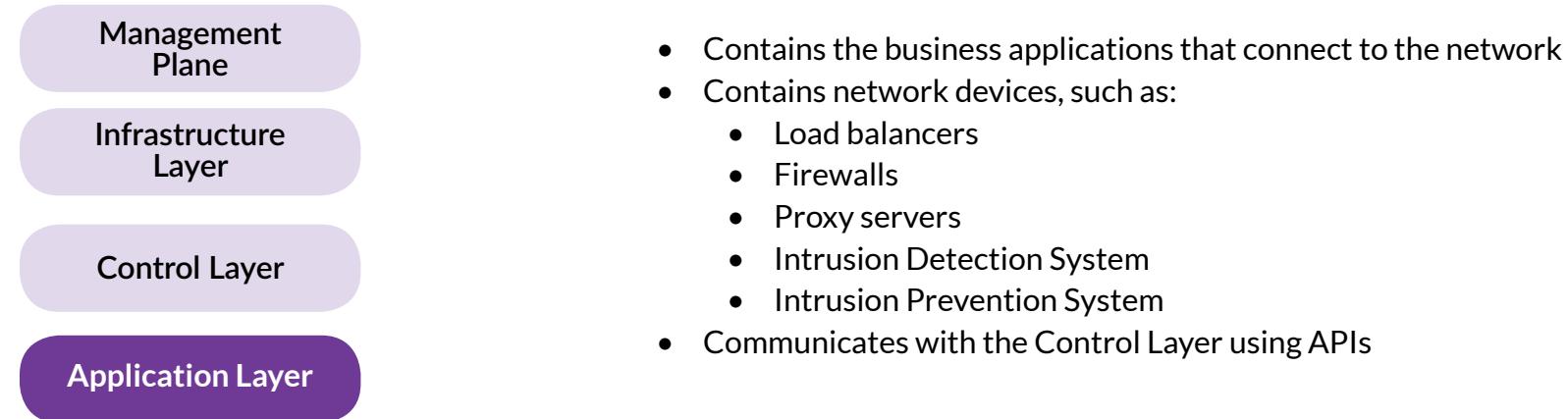


## Software Defined Networking | NTT Global Networks

Networks are becoming complex by having several types of network devices, servers, switches, and large number of packets floating either internally or in and out of the network. The networks can be multi-tiered or layered, which makes the network administrator's job more difficult. Software-defined Networking or SDN simplifies the network management, which otherwise would have been difficult. SDN uses abstractions at each layer of the network to simplify its management. For example, there can be variety of technologies that may be implemented in a network. SDN uses specific applications to control the underlying technologies without having to worry about their complexities.

SDN does not depend on any proprietary technology. Rather, it uses the Application Programming Interfaces (APIs) for programming the network functionalities. Because of its independence from any proprietary technologies, SDN enables the network administrators to integrate different vendor technologies. With its capability to use applications to manage the technologies, there is less complexity. You can use any vendor's technology, but it does not add any complexities. SDN also does not depend on any proprietary protocol and therefore, it makes a good use of the open protocols.

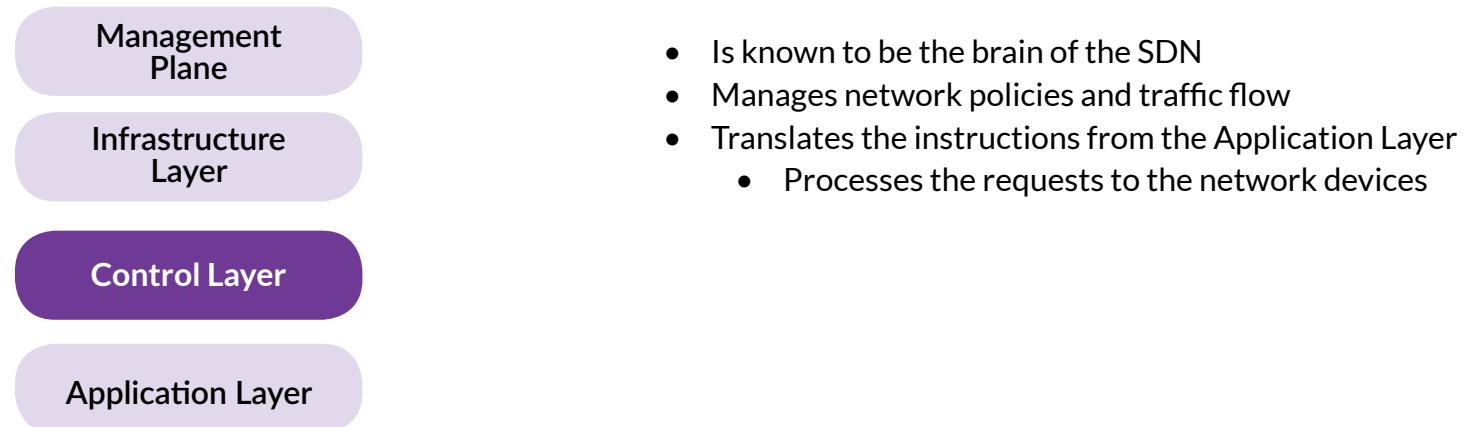
# Application Layer



The SDN architecture contains four core layers. The first layer is the application layer. It contains the applications that connect to the network. Other than the applications, the application layer also contains several network devices, such as load balancers, firewalls, proxy servers, intrusion prevention systems, and intrusion detection systems. The application layer communicates with the layer above, the control layer, with the use of application programming interfaces (APIs).



# Control Layer



- Is known to be the brain of the SDN
- Manages network policies and traffic flow
- Translates the instructions from the Application Layer
  - Processes the requests to the network devices

The control layer is the central controller of the entire SDN. It is known to be the brain of SDN.

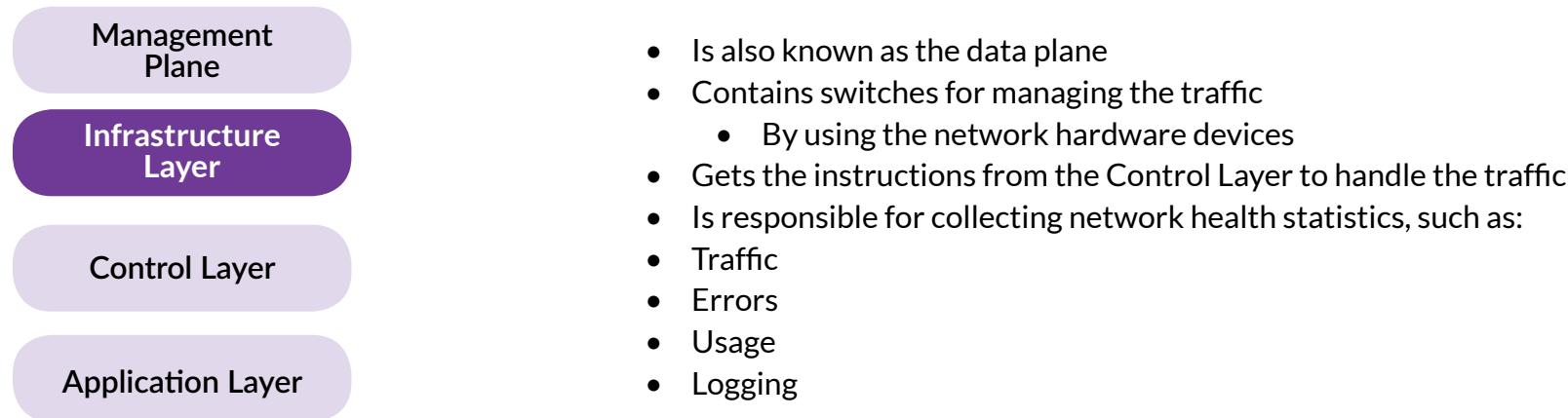
The control layer contains the SDN Controller, which is responsible for the following:

- Process configuration
- Monitoring the SDN

The control layer is situated between the application and the infrastructure layer. The application layer sends the requests to the control layer, passing them to the infrastructure layer. It also sends the information back from the networked devices to the application layer.



# Infrastructure Layer



The infrastructure layer is also known as the data plane. The infrastructure layer receives the instructions from the control layer that define how the traffic needs to be handled. The infrastructure layer consists of several switches responsible for managing the network traffic. The leaf switches are located on the infrastructure layer that receive information and commands from the control layer – the SDN Controller to be precise. Based on the policies of the SDN Controller, the infrastructure layer performs the packet forwarding.

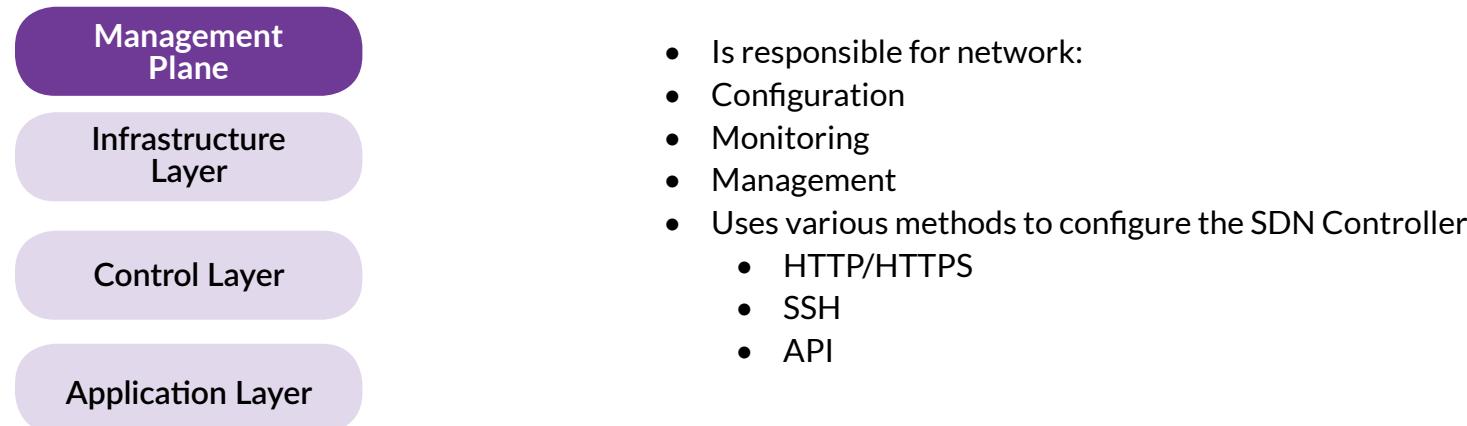
The infrastructure layer is responsible for collecting network health information, which can include:

- Traffic
- Errors
- Usage
- Logging

The network health statistics that it collates, it shares it with the control layer.



# Management Plane



The management plane layer is the one that manages and maintains the SDN network. It has several responsibilities, such as configuration, monitoring, and management of the SDN network. This is the layer using which you perform the SDN Controller configuration. You can use various methods to configure the SDN Controller. These methods are:

- HTTP/HTTPS
- SSH
- API



*TOPIC 3*

---

# SPINE AND LEAF

---

# Spine and Leaf

Backbone

Top-of-rack  
Switching

Spine and Leaf

- Is a two-tier network architecture
  - Spine
  - Leaf
- Offers many benefits, such as resiliency, performance, low latency, scalability, and adaptability
- Spine
  - Contains the high-speed switches
    - Provide high-throughput
    - Offer low latency
- Leaf
  - Are connected with the systems and servers
  - Has each switch connecting to all spine switches

Networks can be designed with several tiers. One of the most commonly used network architecture is the spine and leaf network architecture, a two-tier network architecture. The two tiers consist of a spine and leaf.

Let's look at what spine is. It is the backbone of the two-tier network. It contains high-end switches that are responsible for routing. Because there are no more tiers in between, the switches provide high-throughput and low-latency. They can offer speed from 40 to 300 Gbps.

The leaf tier contains the switches that connect to the rest of the network devices and servers. They receive the data from them and then route it to the switches located in the spine tier. The leaf switches is configured with dual connectivity – one with a network device or server and another one with the spine switches.



# Top-of-rack Switching

Backbone

Top-of-rack  
Switching

Spine and Leaf

- Keeps the access or the leaf switches on top of the rack
- Provides the advantage of low cabling
- Restricts the cables within the rack
- Requires each leaf switch to connect to the spine switches
  - Forms a full-mesh switch network
  - Does not require a leaf switch to connect to another leaf switch

The servers are housed in a server rack. They usually connect to the switches either through the patch panel or through long Ethernet cables. In the Top-of-rack method, the leaf switches are placed on the top of the rack so that the servers can directly connect to them. When servers connect to the leaf switches placed on top of the rack, there are several benefits. The first benefit is that there is low cabling. You need to connect the server directly to the leaf switch. The second benefit is that the cables are restricted within the rack.

The leaf switches need to further connect with the spine switches. The leaf switches form a full-mesh network by connecting to every spine switch, which. The important thing to note is that the leaf switches only connect with the spine switches, not with the other leaf switches.



# Backbone

Backbone

Top-of-rack  
Switching

Spine and Leaf

- Are high-speed switches that connect to the leaf switches
- Does not directly connect with the servers or systems
- Can connect to the network devices
- Can have =>10G interfaces
- Are implemented with redundancy

The backbone switches are usually the spine switches that have connections with the leaf switches. In the previous slide, you learned that the servers connect with the leaf switches. Keeping that thought in mind, it should be obvious that the servers do not connect with the spine switches. It is only the leaf switches that connect with the spine switches.

However, even though servers do not connect with the spine switches, but various other network devices, such as routers and firewalls, can connect with them. The backbone or spine switches have 10 G or higher speed network interfaces. Because the spine switches work as the backbone, they need to be highly redundant





*TOPIC 4*

---

# SPINE AND LEAF

---

# North-South

East-West

North-South

- Is the ingress or egress traffic
  - Moves in and out of a datacenter
  - Moves vertically in a network
- Is filtered by the edge devices, such as:
  - Router
  - Firewall
- Southbound
  - Is the traffic entering a network
- Northbound
  - Is the traffic leaving a network

Let's look at the second case first. In a datacenter, there are two types of traffic. The first type is the traffic that remains within the datacenter and the second type is which flows in and out of the data center. When you have traffic in and out of a data center, it is vertical traffic. For example, a Web server hosted in a data center will deal with the vertical traffic – it will receive traffic from external users on the Internet and send the traffic back to the Internet. This is known as North-South traffic.

The North-South traffic is filtered by the edge devices, such as routers and firewalls.

The southbound traffic is something that enters into a datacenter from the outside world. The traffic that is going out of the network is the northbound traffic.



# East-West

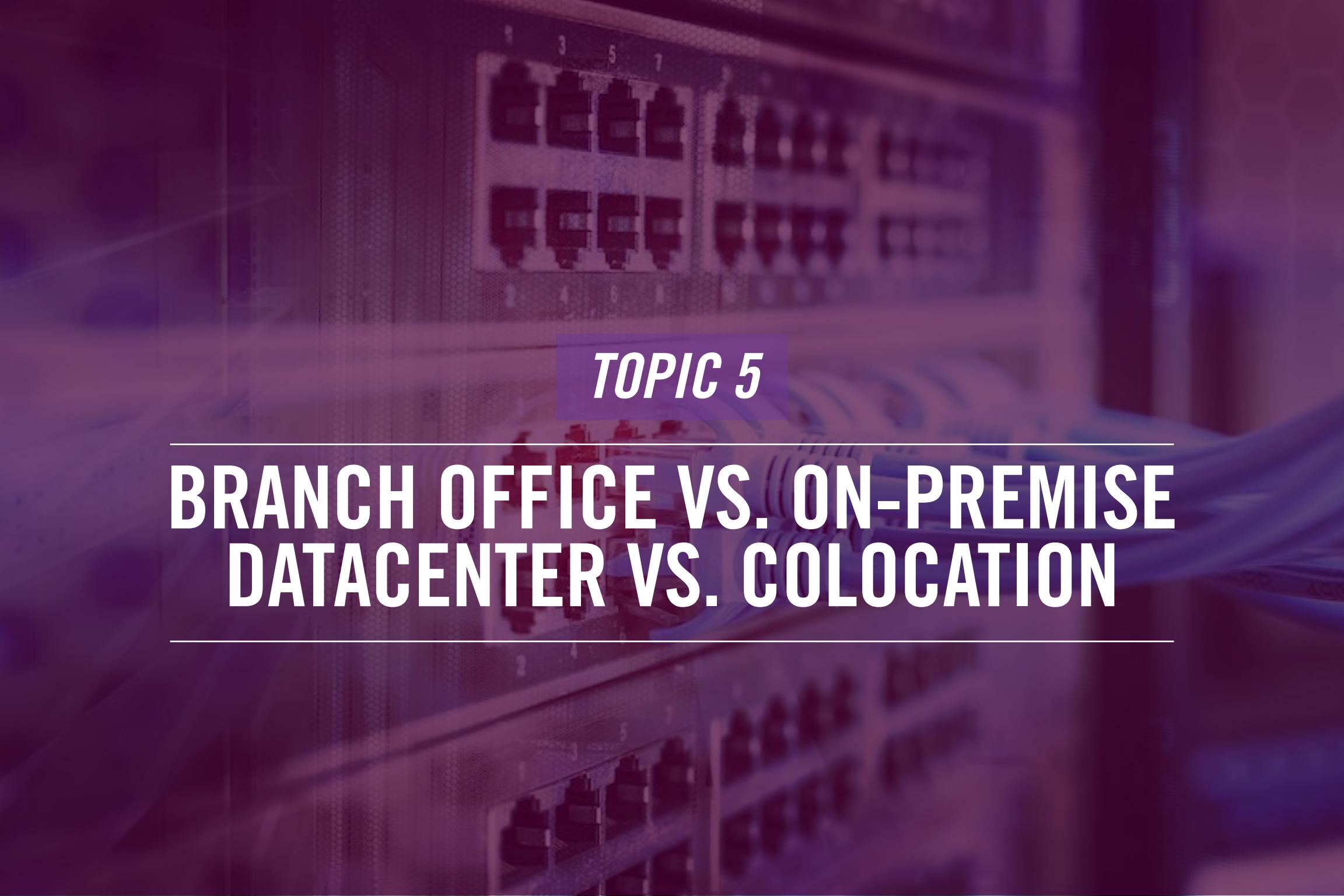
East-West

North-South

- Is the traffic that is flowing within a network
- Is horizontal in nature
- Occurs at the same layer in a network
- Can also be between:
  - Two physical devices
  - One physical and one virtualized device

You just learned about the North-South traffic, which is egress and ingress traffic into a datacenter. Then, you have traffic that stays within the data center and never leaves. It originates from applications or devices within the datacenter and is transmitted to the other applications or devices. Such traffic is horizontal and usually occurs at the same layer in the network. For example, you may have two virtual machines that are communicating with each other. It could also be two physical devices, such as routers. On the other hand, it could be one physical and one virtual device.





## *TOPIC 5*

---

# BRANCH OFFICE VS. ON-PREMISE DATACENTER VS. COLOCATION

---

# Branch Office vs. On-premises Datacenter vs. Colocation

- Branch
  - Uses a distributed network approach
  - Locates some servers, such as authentication, at the branch office
  - Saves on bandwidth
- On-premises
  - Uses a centralized network approach
  - Connects with branch office using any form of connectivity, such as leased lines
  - Provides centralized control of the infrastructure
- Colocation
  - Requires the use of a third-party physical location for infrastructure
  - Is used due to space constraints

There are different ways to architect a network. The network architecture is mainly driven by the business needs of an organization. For example, if an organization is situated in a single location, then you may have on-premises datacenter.

Let's look at the various options for a datacenter. The first approach is the branch office datacenter. You would have a data center in your main office and part of it in the branch office. This is the distributed architecture. The main office needs to be connected with the branch office through leased line or maybe a VPN. However, having a partial data center at the branch office is to reduce the dependency on the primary office datacenter. For example, you can offload the authentication servers in the branch office so that the users can be authenticated at the branch office. Else, the entire authentication traffic needs to reach the main office data center. With offloading a partial data center at the branch office, you eventually save on the network bandwidth and have less dependency. This approach works best when you have less reliable network connectivity between the main and branch offices. Even with the no connectivity with the main office, the branch offices can continue to function.

The on-premises approach is instead centralized. Every single IT function is situated in the centralized datacenter. With the on-premises approach, the organization retains the control of all IT functions. There may be branch offices that need to connect with the main office. In such a scenario, the branch offices connect using leased lines or the VPN services.

The third approach is the colocation approach. In this approach, an organization uses a third-party facility to house its IT infrastructure. The third-party facility is also shared by other organizations and therefore, it is called the colocation approach. Organizations usually use this approach due to physical space constraints.



*TOPIC 6*

---

# STORAGE AREA NETWORKS

---

# Connection Types

- Fibre Channel
  - Connects servers to the SAN
  - Is not compatible with IP network
- Fibre Channel over Ethernet (FCoE)
  - Connects servers to the SAN
  - Does not use the IP network
- Internet Small Computer Systems Interface (iSCSI)
  - Is used for encapsulating the SCSI commands within IP packets
  - Allows the SAN to use the same IP network

A SAN or storage area network consists of various storage devices that connect with each other. Depending on the configuration of the SAN, the devices may be restricted to communicate within SAN or can also communicate with the other devices on the network. A SAN can be limited to a single site or span over multiple sites. A SAN may contain devices like storage devices and servers to serve the need of the users. SANs are fast, fault-tolerant, and can store large volumes of data for an organization. Due to their built-in capabilities for the storage needs, they are often deployed when you need high reliability and fault tolerance.

A SAN can use various connection methods. Fibre Channel is used as the network transmission method to connect servers to a SAN by default. Fibre Channel does not use TCP or UDP. It is a Transport layer protocol used for connecting SAN to another network. There are different ways to implement Fibre Channel, such as Point-to-Point (FC-P2P) that connects two devices directly. It is limited to only two devices. Then, you have Arbitrated Loop (FC-AL), which forms a token ring network. You also have Switched fabric (FC-SW) that works like an Ethernet network where all SAN devices are connected to the Fibre Channel switches.

Fibre Channel over Ethernet (FCoE) encapsulates the Fibre Channel frames an existing Ethernet network. Using FCoE, the existing Ethernet network equipment can be used, but you can also leverage the high speed of the Fiber Channel. For example, you have servers that are running on an Ethernet network. However, they are connected to the FCoE switches. The FCoE switches are further connected to the SAN network. In this way, you still use the existing Ethernet network but use the FCoE protocol to allow the servers to connect to the FCoE switches.

Then, you have the Internet Small Computer Systems Interface, iSCSI. It is a Transport layer protocol that uses TCP for fast data transmission. The data transmissions can be anywhere, on a LAN, WAN, or even on the Internet, which may occur within a LAN, over the WAN, or the Internet. The iSCSI protocol encapsulates the SCSI commands within IP packets, which allows the SAN to use the same IP network.

# Summary

- Three-tiered
- Software-defined Networking
- Spine and Leaf
- Traffic Flows
- Branch Office vs. On-premises Datacenter vs. Colocation
- Storage Area Networks

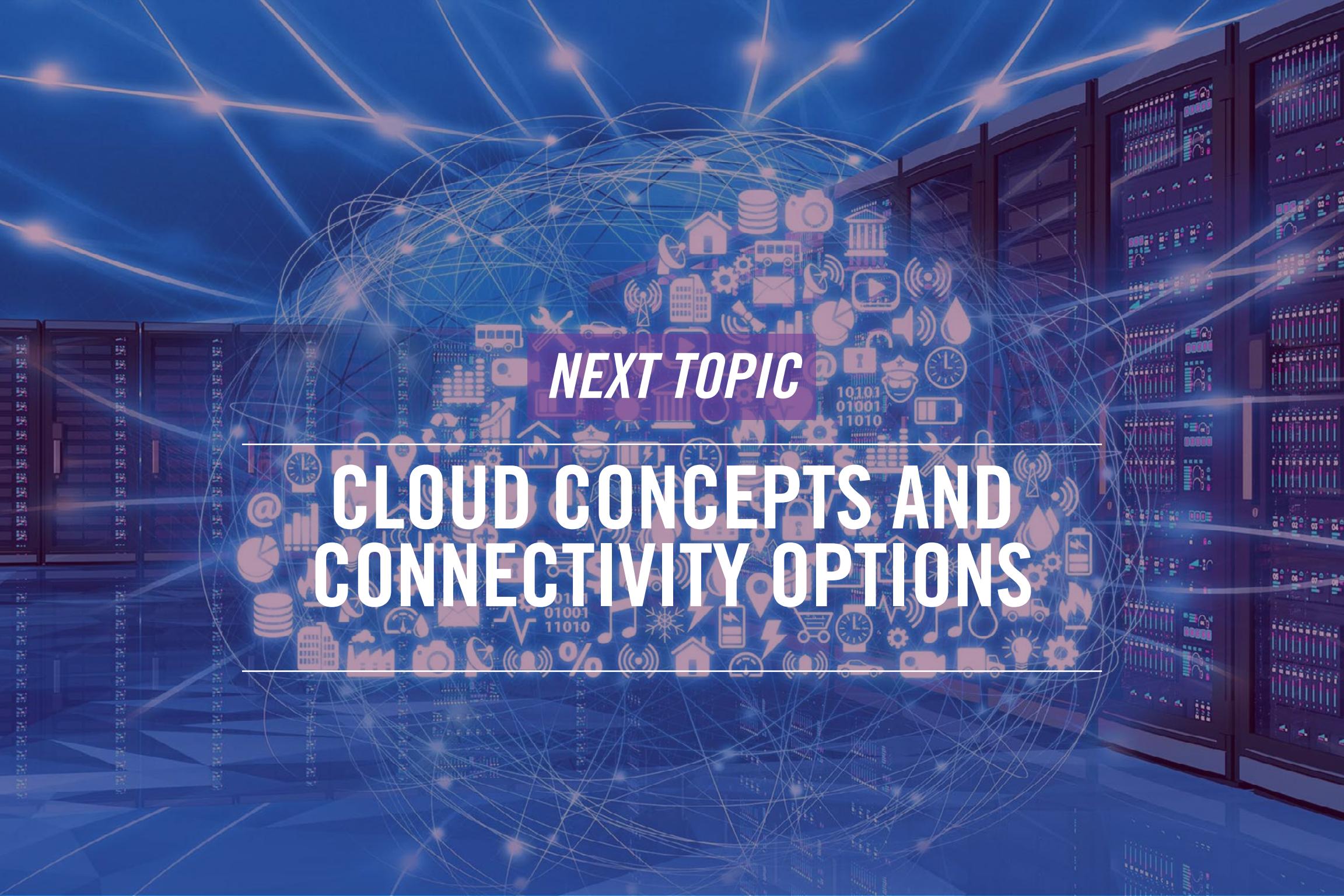


That's the end of the lesson.

Here we covered:

- Three-tiered
- Software-defined Networking
- Spine and Leaf
- Traffic Flows
- Branch Office vs. On-premises Datacenter vs. Colocation
- Storage Area Networks





*NEXT TOPIC*

---

# CLOUD CONCEPTS AND CONNECTIVITY OPTIONS

---

Lesson

8

# Cloud Concepts and Connectivity Option

- 1 — Welcome to the lesson 8 of Module 1. In this lesson, you will learn about the:
- 2 — Cloud concepts and connectivity options.



Network Fundamentals

# Agenda

- Deployment Models
- Service Models
- Infrastructure As Code
- Connectivity Options
- Multitenancy
- Elasticity
- Scalability
- Security Implications

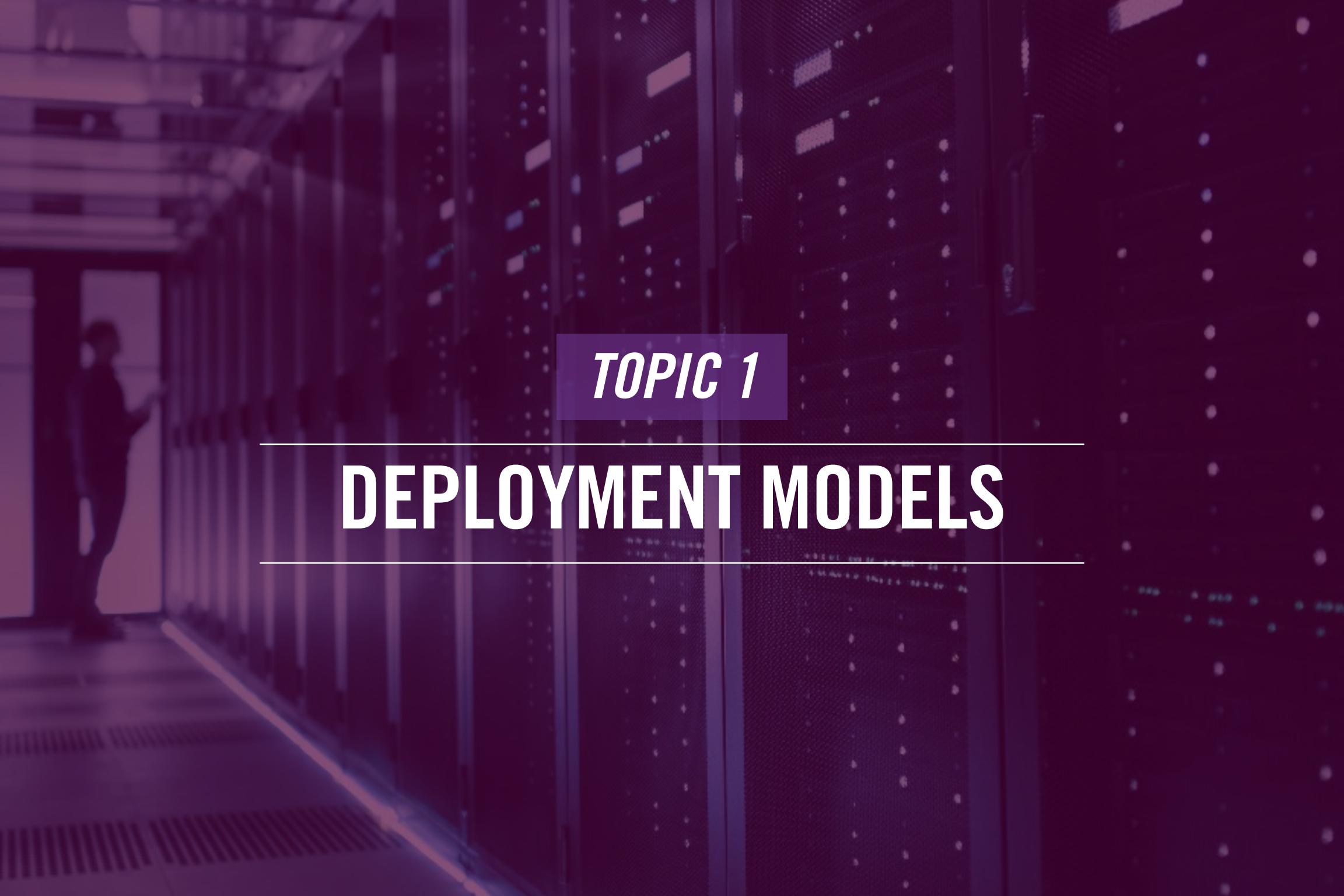


Hi, welcome to COMPTIA Network+ Course

In this lesson, we will talk about:

- Deployment Models
- Service Models
- Infrastructure As Code
- Connectivity Options
- Multitenancy
- Elasticity
- Scalability
- Security Implications





*TOPIC 1*

---

# DEPLOYMENT MODELS

---

# Public Cloud

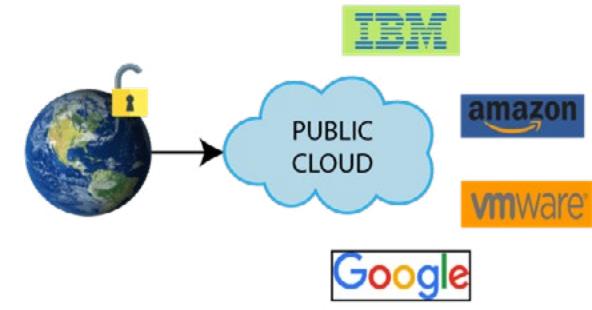
Hybrid

Community

Private

Public

- Works on the shared infrastructure
- Requires users to pay by:
  - Subscriptions
  - Pay-per-use
- Is owned by a third-party service provider
- Is cost-effective and easier to maintain
  - Users have zero-maintenance on the infrastructure
- Is less secure than the private cloud



The public cloud is probably the most used cloud delivery model. It works on shared infrastructure. When you refer to the shared infrastructure, it is an infrastructure that several cloud customers use simultaneously. For example, two or more organizations may be using the same servers in the backend. However, cloud customers never come to know this.

Depending upon what you are using, the public cloud may charge based on subscriptions or pay-per-use, which essentially means that you pay for what you use. A third-party cloud service provider owns a public cloud. Amazon EC2, Google Cloud Platform, and Microsoft Azure are public clouds that offer a set of services to cloud customers.

For organizations, a public cloud is a cost-effective solution. Whether getting 100s of copies of Office 365 or setting up a new network, a public cloud provides both options with minimum costs. Also, the customer does not have to maintain the infrastructure. It is the responsibility of the cloud service provider to maintain the infrastructure and the hardware running in the backend.

Because a public cloud works on shared infrastructure, it is less secure than a private cloud, which you will learn about in the next slide.

# Private Cloud

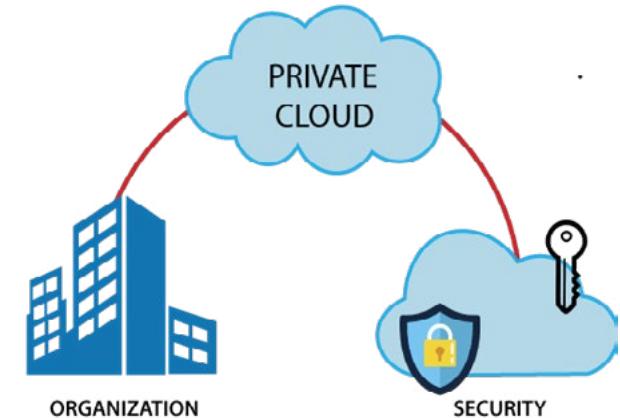
Hybrid

Community

Private

Public

- Is set up by an organization or by a third-party for the organization
- Is dedicated to a single organization
  - No shared infrastructure
- Is more expansive than public cloud
- Provides higher security than public cloud
- Provides more flexibility in configuration



[Private Cloud - javatpoint](#)

A private cloud is either set up by an organization or a third party for an organization. A private cloud is dedicated to a single organization that runs its infrastructure. No other organization or entity is sharing the cloud with the organization that owns the cloud.

A private cloud is usually more expensive than a public cloud in terms of cost. The reason is that you have to put up your cloud by setting up the infrastructure that will host the private cloud.

Since there is no shared infrastructure, a private cloud is more secure than a public one. Of course, it depends on the organization to beef up the security – the more layers of security you add, the more secure the private cloud becomes.

When dealing with the private cloud, you control the complete infrastructure, including the hardware. Therefore, you have the flexibility to add or remove devices, hardware, and software.

# Community Cloud

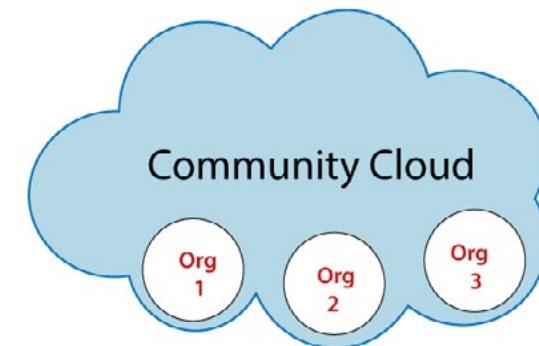
Hybrid

Community

Private

Public

- Has the same set of resources shared by multiple entities
- Works well with the entities, such as federal agencies, that share common characteristics
  - Security
  - Privacy
  - Compliance
- Example:
  - IBM SoftLayer
  - Salesforce Community Cloud



[Community Cloud - javatpoint](#)

A community cloud uses the same set of resources shared by multiple entities with similar nature of the business or a common goal. It could also be that they may have similar security requirements, privacy needs or comply with a specific regulation.

For example, federal agencies in the United States of America cannot use the public cloud for sharing confidential data. It is not cost-effective for them to put private cloud. The solution is to use the community cloud, allowing them to use the same infrastructure and resources.

Two key examples of community cloud are IBM SoftLayer and Salesforce Community Cloud.

# Hybrid Cloud

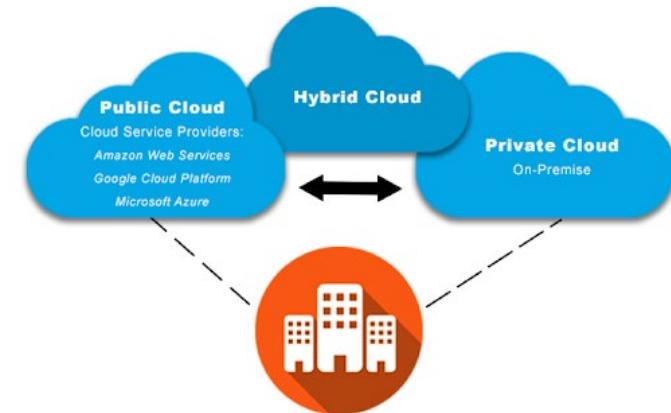
Hybrid

Community

Private

Public

- Combines public and private cloud
- Provides flexibility and security
  - Flexibility using the public cloud
  - Security using the private cloud
- Can be used for high performance applications



[Public Cloud Vs Private Cloud Vs Hybrid Cloud | Nutanix](#)

There may be a situation when you need to have the flexibility of the public cloud and the security of a private cloud. Consider a financial institution that cannot host confidential data in the public cloud. The answer to their requirement is a hybrid cloud. They can host the front-end application in the public cloud, but the backend database remains in the private cloud. In a nutshell, you are leveraging the powers of a private and public cloud.

A hybrid cloud is typically used when you need to host high-performance applications that can demand many resources as they are hit with the volumes of requests. It may not be easy to cater in a private cloud, but the public cloud offers the flexibility of scaling up and down as and when required.

*TOPIC 2*

---

# SERVICE MODELS

---

# SaaS

DaaS

PaaS

IaaS

SaaS

- Is used for hosting applications in the cloud
- Provides access to the users based on subscription
- Requires a Web browser to access applications
- Examples: Gmail, Office365



[True Cloud Story About: IaaS, PaaS & SaaS | by Mohammed Albihany | Medium](#)

If you have ever used Office 365 or Gmail or, in fact, any other cloud-hosted application, maybe a Customer Relationship Management (CRM) application, you have already experienced SaaS or Software as a Service delivery model.

In SaaS, an application is hosted in the cloud environment and is made available to the users who have to purchase a subscription. Some part of the application may be made available free of cost, or the application may be free to use for a certain period. However, the users have to purchase the subscription to use the full set of features, or their trial time is over.

The SaaS applications are accessible using a Web browser. In some cases, like Office 365, you may have a downloadable application, but it is connected to the SaaS platform in the backend. It keeps track of your subscription, and if it expires, you can no longer use the application or may be restricted to use fewer features.

Key examples of SaaS are Gmail, Office 365, and Dropbox.

# IaaS

DaaS

PaaS

IaaS

SaaS

- Allows the network administrators to set up their networks in the cloud
- Works just like the on-premise infrastructure except the access to the physical hardware
- Allows upscaling and downscaling as and when required
- Works in the pay-per-use model
- Example: Amazon EC2, Microsoft Azure

## IaaS



[True Cloud Story About: IaaS, PaaS & SaaS | by Mohammed Albihany | Medium](#)

You are a startup organization and don't have the funds to set up a complete network, which requires upfront cost – you pay and buy the hardware and software. With IaaS, or Infrastructure as a Service, you are not required to pay upfront. You can set up the entire infrastructure in the cloud, which will work like on-premises infrastructure, except that you will not have any control over the hardware.

Using IaaS, you can set up virtually any device or virtualized hardware in the cloud environment. You can simulate the entire network in the cloud and scale it up or down as and when required. You can add more servers on the fly, and a few hours later, you can even release them if you don't need them. You can create virtual machines, install operating systems, and even take backups.

The IaaS model works with the pay-per-use model. You pay only for what you use, which is not the case with the on-premises hardware – once you have bought it, whether you use it or not, you have already paid for it.

Key examples of IaaS are Google Cloud Platform, Amazon EC, and Microsoft Azure.

# PaaS

DaaS

PaaS

IaaS

SaaS

- Provides development platform the programmers and developers
- Hosts development tools
- Reduces the cost of development tools for the developers
- Example: Google App Engine, Microsoft Azure, Intel Mash Maker



[True Cloud Story About: IaaS, PaaS & SaaS | by Mohammed Albihany | Medium](#)

The Platform as a Service or PaaS is intended for developers. It provides a development environment for the programmers and developers.

PaaS hosts a variety of development tools. For example, you can develop mobile applications to develop applications in Python or Java.

The developers do not need to purchase and install the development tools on their systems with the PaaS. They need to connect to PaaS and start using the development environment as they would have done it on their systems.

Everything is readily available for them to start coding. They need to log on to their accounts and write the code.

Some of the key examples of PaaS are Google App Engine and Microsoft Azure.

# DaaS

DaaS

PaaS

IaaS

SaaS

- Is Desktop As A Service
- Provides virtual desktop to the users via a Web browser
- Uses the per-user subscription model
- Can be either:
  - Persistent
  - Non-persistent



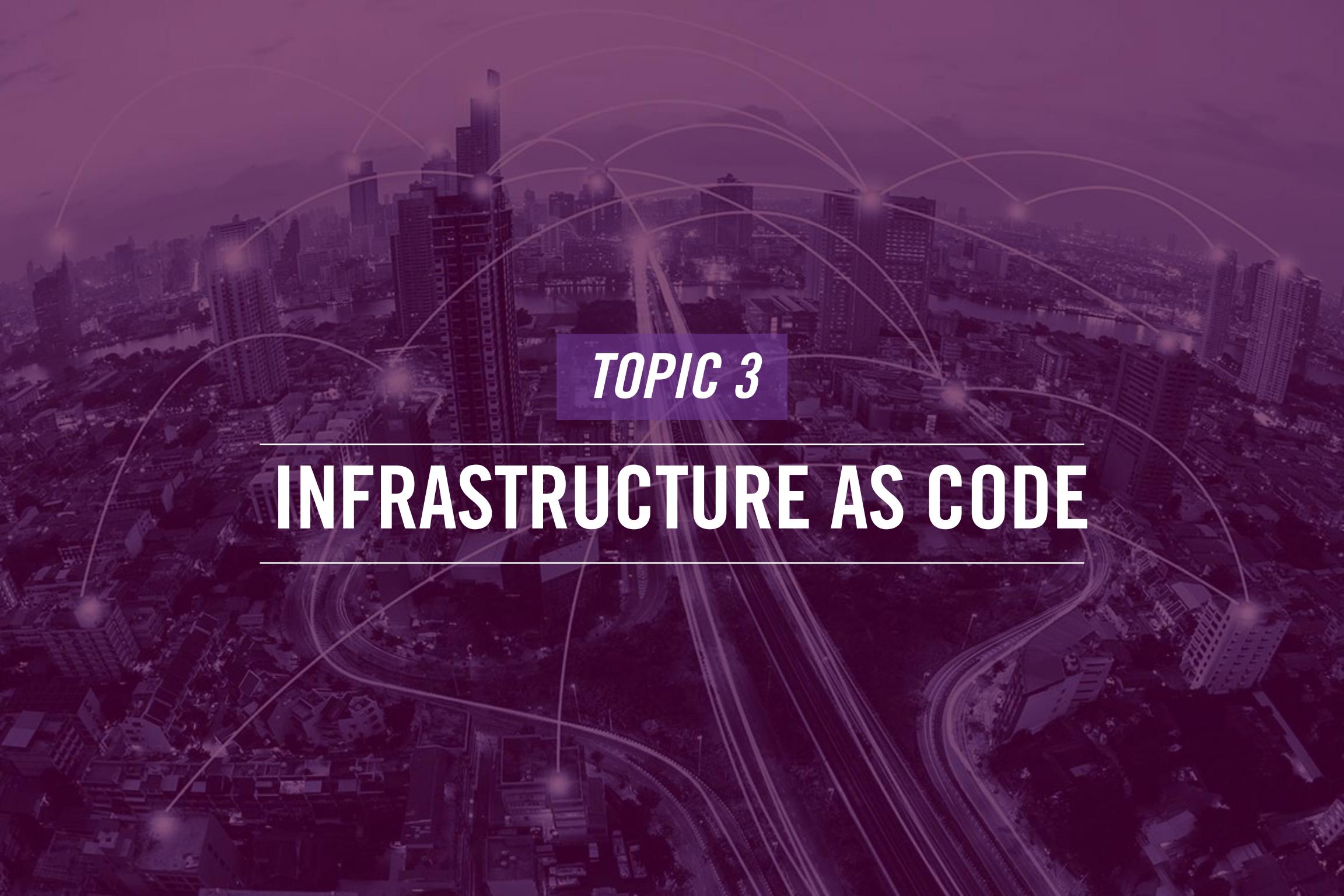
[The Benefits of Desktop-as-a-Service \(DaaS\)?Sangoma](#)

DaaS is a Desktop as a Service that a cloud service provider hosts. A virtual desktop is provided to the user to connect to the cloud environment via a Web browser and start working as if they are working on their system.

The cloud service provider is responsible for managing the DaaS infrastructure. It is good for the organizations that do not have readily available cash to set up a virtual desktop infrastructure.

DaaS environment provides two options for the users:

- Persistent: A user sets it up and saves the settings. The settings are reflected when the user logs back in after a logout.
- Non-Persistent: As the user logs out, all settings are wiped out. A standard desktop is displayed to the user when he logs back in.



## *TOPIC 3*

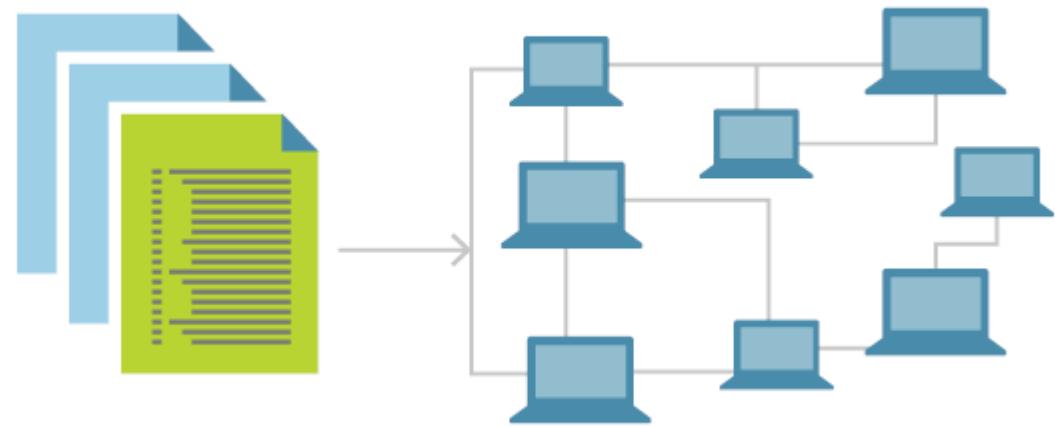
---

# INFRASTRUCTURE AS CODE

---

# Infrastructure As Code (IaC)

- Use a high-level descriptive coding language to set up the infrastructure
- Automates the provisioning of infrastructure
- Removes the manual work to:
  - Set up and manage servers
  - Installing operating systems
  - Configuring storage and databases
- Helps to orchestrate across multiple systems
  - Span a distributed application across several systems

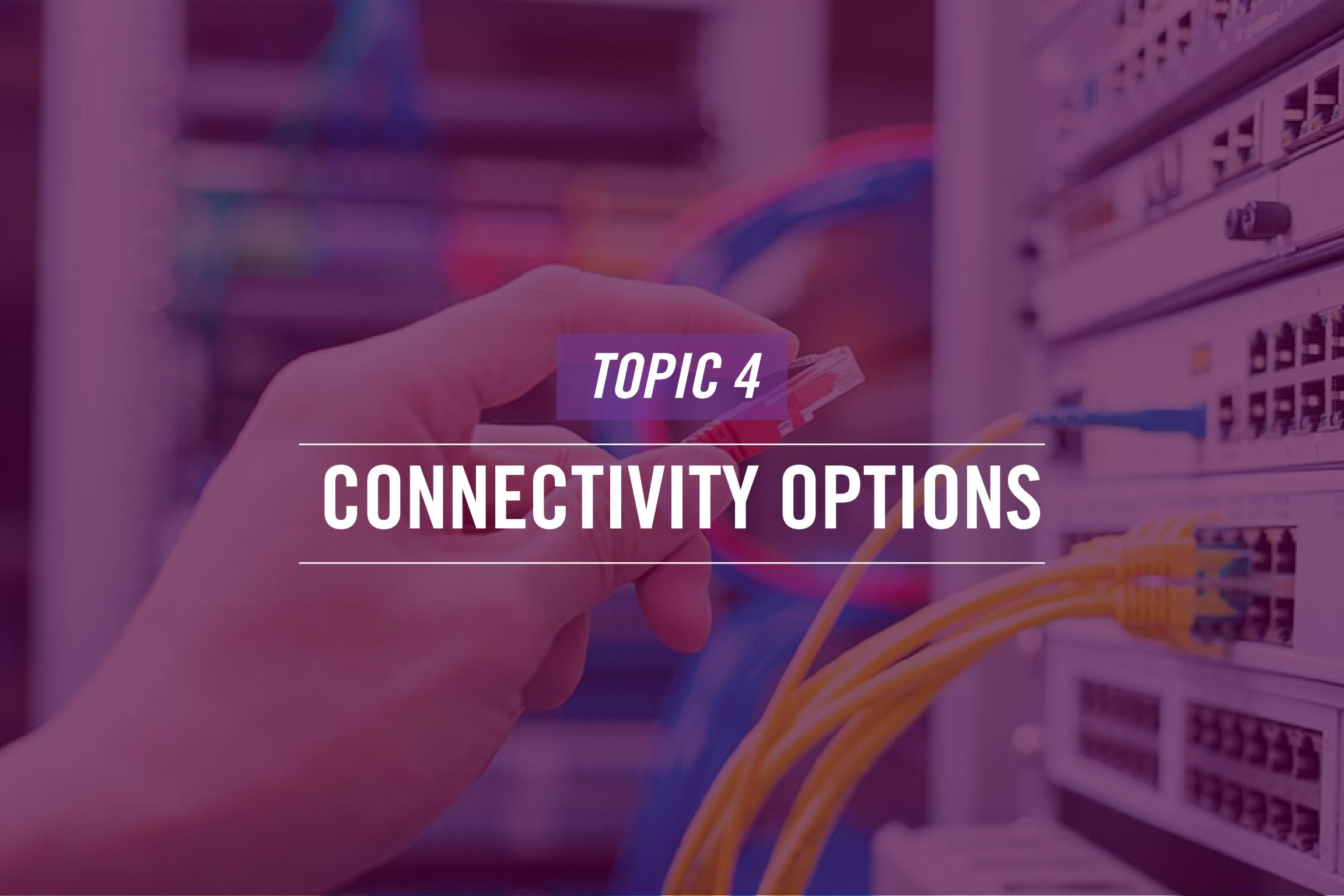


[What is Infrastructure as Code? - Azure DevOps | Microsoft Docs](#)

When a developer needs to write code to develop an application, much time is spent setting up the infrastructure. It could be the servers, systems, applications, and so on. This usually takes from a few hours to a few days.

To resolve this problem of setting up the infrastructure, cloud environments help the users build up their infrastructure within a few minutes using a high-level descriptive coding language. With the use of this language, you automate the provisioning of the IT infrastructure. This removes the manual work of setting up or provisioning the IT infrastructure, including various tasks, such as setting up servers, installing operating systems, and configuring the storage and database.

Using IaC, you can orchestrate across multiple systems. If you need to work on a distributed application, you can span it across several systems within no time. With IaC, what you achieve is speed and consistency, which eventually help you save costs. Considering someone spending a week setting things up and then being replicated on another site, it is another week. All this can be done in a few minutes and save manpower.

A close-up photograph of a person's hands holding a red Ethernet cable with a RJ45 connector. They are positioned over a server rack with several blue and yellow cables already connected to it. The background is slightly blurred.

*TOPIC 4*

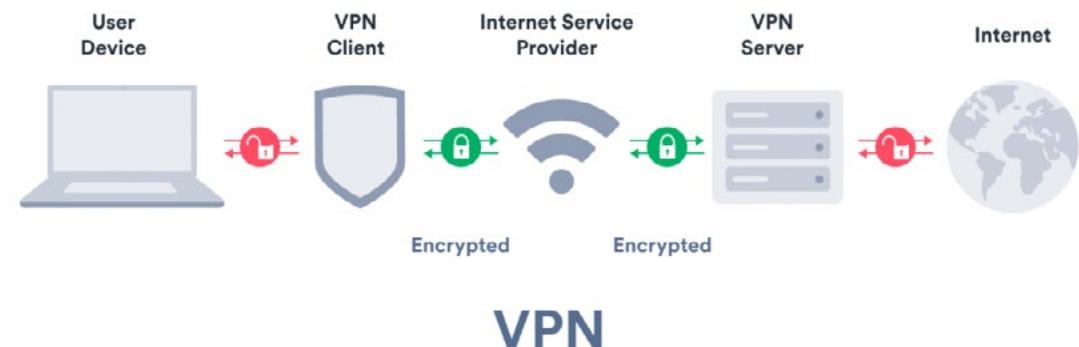
---

## CONNECTIVITY OPTIONS

---

# Virtual Private Network (VPN)

- Site-to-site VPN:
  - Is between VPN gateway in the cloud and a VPN endpoint in on-premises
  - Joins two networks over the internet.
  - Uses IPsec
- Client-to-site VPN:
  - Is between a VPN gateway in the cloud and a VPN client



[What is VPN? Virtual Private Networks 101 - Surfshark 2022](#)

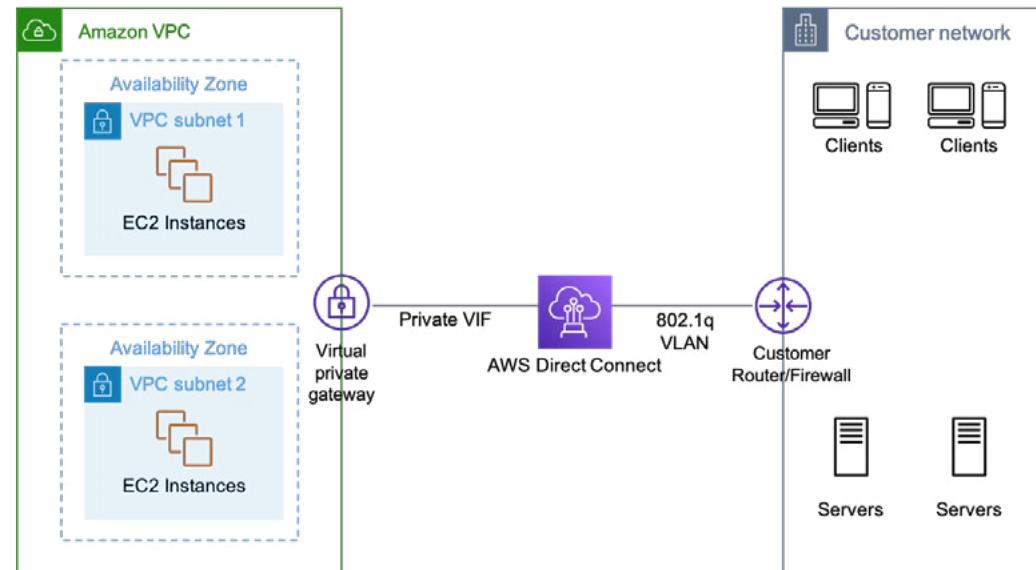
You must have used VPN earlier to connect to your office network. With the cloud environment, you get two options. You can either use the site-to-site VPN or client-to-site VPN.

The site-to-site VPN requires connecting two sites, on-premises, and the cloud environment. A VPN gateway in the cloud is configured to accept connections from the onsite or on-premises VPN server or endpoint that has VPN configured. When you configure site-to-site VPN, both the sites have access to each other except for what you block or restrict using access control lists. Site-to-site tunnels are encrypted using IPsec.

The client-to-site VPN has one VPN gateway in the cloud, and the clients are installed on the users' systems. A client initiates a connection to connect to the VPN gateway, and after being authenticated, the user is authorized to access cloud resources.

# Private-Direct Connections

- Is a dedicated direct connection between:
  - The cloud environment
  - Customer's network
- Creates the IPSec-encrypted private connection between two endpoints



[AWS Direct Connect - Amazon Virtual Private Cloud Connectivity Options](#)

You can connect your on-premise infrastructure with the cloud environment using a Private-Direction connection. Connection is established using services like AWS Direct Connect, which connects to the VPN gateway and the client's edge device, a router, or a firewall.

With AWS Direct Connect, for example, you can establish 1 Gbps or 10 Gbps dedicated network connections, which are encrypted using IPSec.

## *TOPIC 5*

---

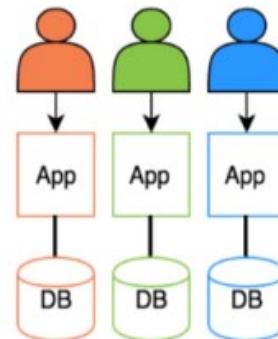
# MULTITENANCY

---

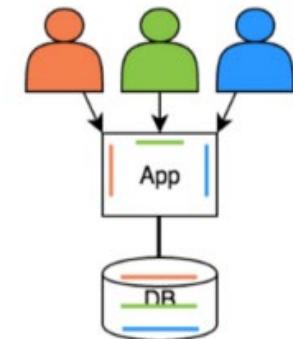
# Multitenancy

- Has several tenants using the same cloud infrastructure
  - The same server or system
  - The same hard drive (for data)
- Is done by the cloud service provider to achieve cost efficiency

Single-Tenant



Multi-Tenant



Vs

[MultiTenancy Architecture - lakshaysuri \(wordpress.com\)](#)

Several tenants share the same infrastructure in the cloud environment, specifically in the public cloud. The software, servers, and storage that the tenants are sharing. The tenants don't know which server is hosting their applications and data, but several still share it.

It is the same server or system or even the same hard drive on a server shared by the tenants. For example, in the IaaS environment, several tenants share the same physical host or system. In the SaaS environment, several tenants use the same application instance.

Multitenancy is mainly used to save the cost of the infrastructure. The cloud service provider also offers single-tenant infrastructure, usually at a high cost.

A close-up photograph of a person's hands pulling apart a large pile of colorful elastic bands (rubber bands). The hands are positioned at the ends of a tangled mass of bands, which are primarily red, yellow, blue, and purple. The background is a solid, dark color.

## *TOPIC 6*

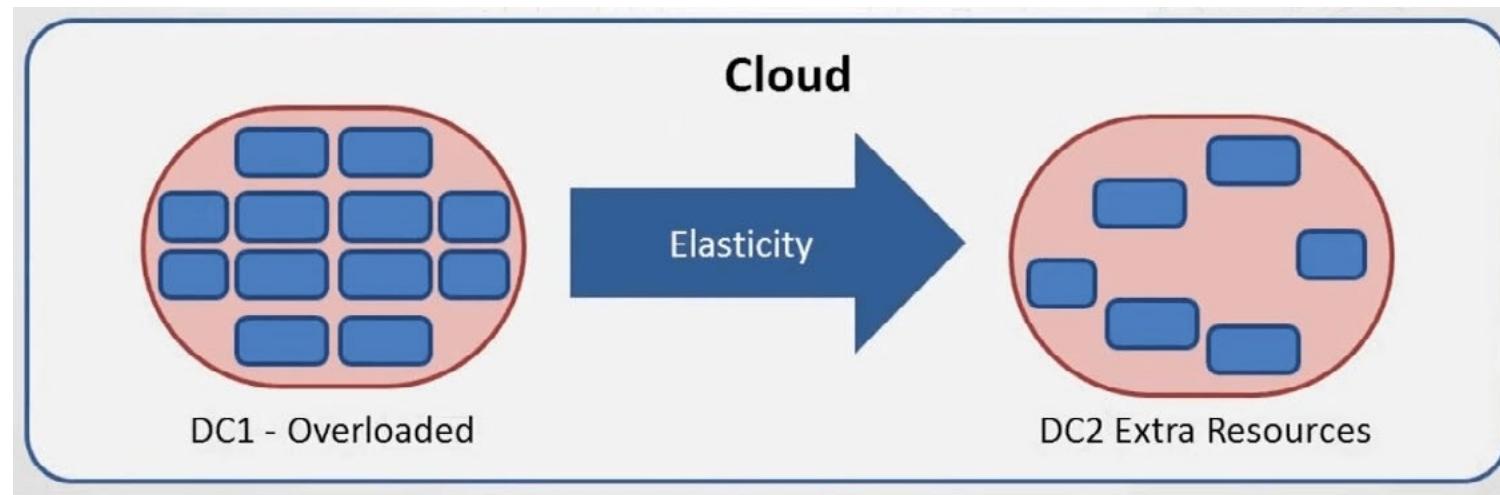
---

# ELASTICITY

---

# Elasticity

- NIST defines Elasticity as:
  - “Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.”



Elasticity, as defined by NIST, is:

“Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.”

In simpler terms, elasticity is about adding or removing resources to your infrastructure in an automated manner. When workload increases, resources are automatically added for the applications that demanded them. When the workload decreases, the resources are automatically removed without any manual intervention. Elasticity helps in controlling cloud resources costs. You have to pay only for what you use. When the resources are not required, it simply removes them.



*TOPIC 7*

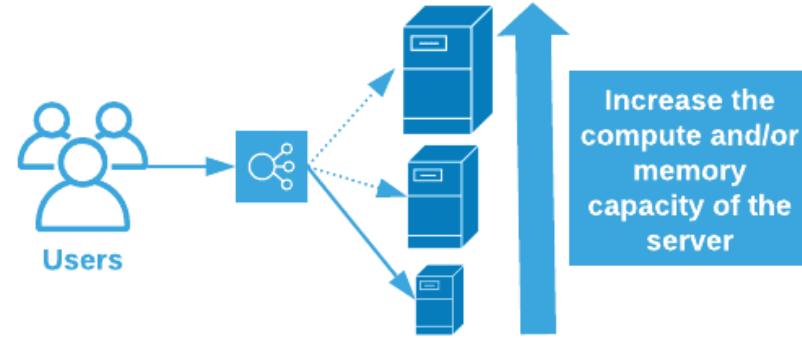
---

# SCALABILITY

---

# Scalability

- Is when the administrators add more resources to get optimal performance
- Is about increasing the resources to manage the load
- Scaling Up
  - Add more resources to the system
- Scaling Out
  - Adding more systems for load management



[What is Scalability in Cloud Computing? | MuleSoft Blog](#)

Each system or server you set up either physically or in the cloud has resources like memory, storage, and processors. The operating systems and applications require these resources. When you need to scale up your systems to meet the demand of the applications, you need to add more resources. You can achieve scalability either by scaling up or scaling out.

The first method is scaling up, requiring you to add more resources within the same system the application is installed.

The second method is to scale out, which requires you to leave the current system but add more systems to load balance the application.

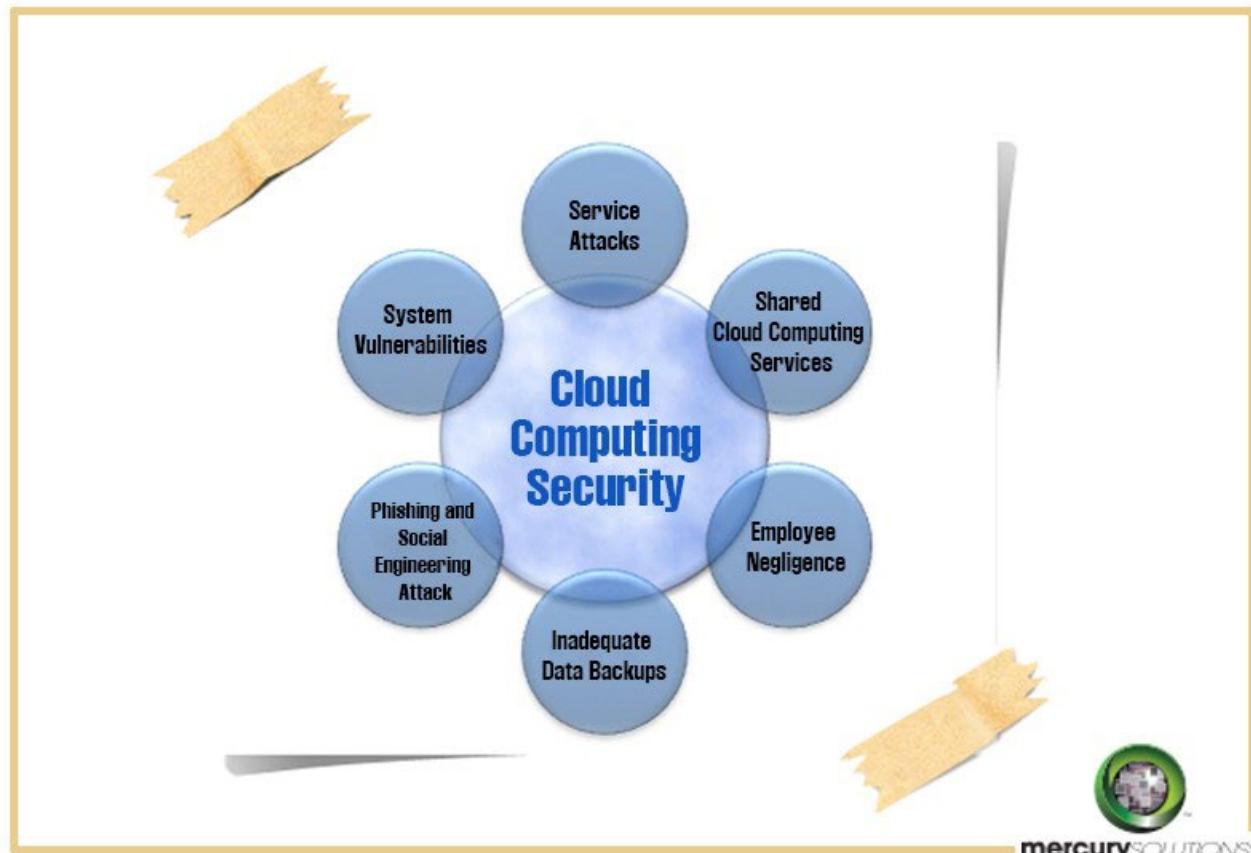
## *TOPIC 8*

---

# SECURITY IMPLICATIONS

---

# Security Implications



[The security issues around cloud computing !! | by Rahul Dwivedi | Medium](#)

# Security Implications

Even though the cloud environment has good offerings and has been highly adaptable by many organizations worldwide, there are still some security implications that cause worry in people's minds. Let's look at some of these security implications.

Many cloud consumers use the public cloud, which works with shared resources. This causes a serious threat. If one of the cloud consumers having data and applications on one server is compromised, the threats become real for the other tenants on the same server.

## Employee Negligence

Most organizations allow their employees to remotely connect to their networks or the cloud applications and data. Nowadays, employees use a mobile phones, tablets, and other devices to connect to the cloud. If any of these is vulnerable or infected with malware, it can also impact the cloud environment.

Data backups can be a concern in the cloud environment. You don't know where your data is replicated and if it is replicated at all. In a cyber-attack, such as malware or ransomware, it might be difficult to retrieve data if the data is not backed up properly.

Specifically, social engineering and phishing have been a threat to cloud environments. If a user accidentally falls to the phishing threat and is connected to the cloud, the attacker can access the user credentials and do the lateral movement to sabotage the cloud infrastructure.

Just like the on-premises infrastructure, cloud infrastructure is also prone to vulnerabilities. After all, it is still running on the physical infrastructure and using the same set of operating systems and applications. A single vulnerability in the operating systems or applications in the cloud can let an attacker exploit the cloud environment.



# Summary

- Deployment Models
- Service Models
- Infrastructure As Code
- Connectivity Options
- Multitenancy
- Elasticity
- Scalability
- Security Implications



That's the end of the lesson.

Here we covered :

- Deployment Models
- Service Models
- Infrastructure As Code
- Connectivity Options
- Multitenancy
- Elasticity
- Scalability
- Security Implications





*NEXT TOPIC*

---

# NETWORKING AND NETWORKED DEVICES

---

---

# MODULE 2

---

# Module 2

- LESSON 1 [NETWORKING AND NETWORKED DEVICES](#)
- LESSON 2 [ROUTING AND BANDWIDTH MANAGEMENT](#)
- LESSON 3 [ETHERNET SWITCHING FEATURES](#)
- LESSON 4 [WIRELESS STANDARDS AND TECHNOLOGIES](#)



Lesson

1

---

# Networking and **Networked Devices**

- 1 — Welcome to the first lesson of Module 2. In this lesson, you will learn about the:
  - 2 — Networking and Networked Devices
- 



Network Fundamentals

# AGENDA

- Networking Devices
- Networkeda Devices



Hi, welcome to COMPTIA Network+ Course

In this lesson we will talk about:

- Networking Devices
- Networked Devices



## *TOPIC 1*

---

# NETWORKING DEVICES

---

# Hub

- Is a Layer 1 or the Physical layer of the OSI model
- Connects several systems together
- Sends the received packet to all ports that have systems connected
- Generates congestion as the traffic is sent to all ports
- Performs no error-checking as it lacks intelligence

**Active Hub**

**Passive Hub**



A hub is a networking device that operates at Layer 1, the Physical Layer of the OSI model. It allows multiple systems to connect for communication. Hubs are more or less obsolete from today's network and have been replaced with switches about which you will learn soon. A hub usually has 4 to 12 ports.

When you connect systems on a hub, they form a single collision domain, a type of network that shares the bandwidth. A hub can form a single network as it cannot be segmented to create one network.

A hub can only work in the half-duplex mode. When a system connected to a hub sends out a message to another system, the message is sent to all the ports. Every system connected to the hub gets the same message. This causes network congestion as a hub uses the shared bandwidth.

You cannot assign an IP address to a hub, and it cannot be managed through a management application or management interface. It is a device that does not have any intelligence. The only purpose it serves is to connect multiple systems or devices.

A hub also cannot perform error-checking. When a system connected to the hub sends out a message, the hub does not check the packets. It simply ignores the contents of the packets and does not check for any errors. It takes the packet and forwards it to all systems connected to different ports. Because a hub does not contain any address table for the connected systems, it does not know which system is the actual recipient of the message. Therefore, it has to forward the message to every other system that is connected.

Hubs can be of two types:

- Active: Uses a power supply to power itself and can work as a repeater. It can analyze the data packets. They can also amplify the signals.
- Passive: Requires no power supply and cannot amplify signals. It just forwards the received packets.

# Layer 2 Switch

- Is a network device that operates on the OSI Layer 2 or the Data Link layer (L2 switches)
- Receives and sends frames based on their MAC addresses
- Sends the traffic only to the required port on which the recipient system is connected
- Builds a CAM table
- Works within a network only



You can consider a Layer 2 switch an upgraded version of a hub, but with many capabilities. Unlike a hub, which works at Layer 1, Physical layer, a switch works at Layer 2, the Data Link layer. However, a switch can also work at Layer 1.

A Layer 2 switch is an intelligent device that has decision-making capability. It uses the Media Access Control (MAC) address to send and receive information.

Before you proceed further, you need to understand that the MAC address is the physical address of a network adapter. It is a 48-bit serial number that is globally unique for every network interface card (NIC).

Now, let's see how MAC address plays a vital role in sending or receiving communication in a Layer 2 switch. You have a switch that has systems connected from port 1 to 24. The system on port 12 sends information to the system on port 12. When the system on port 12 sends the message, the switch refers to the MAC address of the destination system, which is on port 20, and then checks its address table for the MAC address. It then directly routes the message to port 20 without having to broadcast the message to every system. In this manner, the remaining systems are unaware of the communication between systems connected on port 12 and port 20.

It is important to note that the address table in the switch is updated almost every second. When a message arrives at the switch, it searches for the relevant MAC address in the address table. If it finds the MAC address, then it forwards the message to the relevant system. If the MAC address is unavailable, it updates the address table first and then forwards the packet to the respective system.

A Layer 2 switch works only within a network.

# Layer 3 Capable Switch

- Is a network device that operates on the Layer 2+3 of the OSI model
- Can use IP addresses to route the packets
- Communicates within or outside the network
- Can have multiple broadcast domains
- Capabilities depends on vendor and price



A Layer 3 switch is a network device that operates at the Layer 3 or the Network layer of the OSI model. It also can operate at Layer 2 and, therefore, is also known as a multilayer switch. Because of its capabilities to work across the layers, it can act as a switch and a router. It can perform switching like a Layer 2 switch, but at the same time, it can perform routing as a router. It uses the application-specific integrated circuit (ASIC) microchips for routing operations.

Let's talk about an example of a Layer 3 switch. In a typical setup, you will have several virtual LANs (VLANs) connected to a Layer 2 switch, which is then connected to a router. When the traffic needs to flow from one VLAN to another VLAN, it has to travel to the switch and then be routed through the router. This adds latency because the traffic is traveling through two different devices. On the other hand, you can remove the Layer 2 switch and the router and replace them with a Layer 3 switch. When the traffic reaches the Layer 3 switch, it can make the routing decision on its own and route the traffic to the correct VLAN.

However, unlike a Layer 2 switch, it uses IP addresses to identify the connected devices. The data is routed to the destination based on the IP address and subnet mask it has. When a system sends a packet, the Layer 3 switch checks its routing table for the IP address and subnet mask. After it finds the IP address, it forwards the packets to the correct destination. Depending on its destination address, it can send packets to a different VLAN within the network or to a different network. Each port on the switch acts as a single broadcast domain.

# Router

- Is a Network layer, the 3rd layer in the OSI model, device
- Connects two networks together – typically the local area network (LAN) and wide area network (WAN)
- Routes the packets based on the destination addresses from the packet's header
- Has a dynamic routing table
- Does NOT forward broadcasts



As a Layer 3 switch, a router is also a Layer 3, the Network layer, device. A router is an edge device, which means it is placed on the network's edge to connect the local network to the wide-area network (WAN). It has several interfaces that allow you to connect the internal network and the WAN network. The router's job is to pass the traffic from one interface to the other interface.

The main function of the router is to route traffic between networks. When it receives the traffic from one network, it has to make routing decisions to route the packets to the correct destination. The decisioning is made by reading the packet's header to determine the IP address of the destination. When a packet is received at the router, it checks for the packet's header's destination address. Then, it checks for the destination address in its routing table. When the address is found, it forwards the traffic to the correct destination address.

A router acts as a single broadcast domain. Anything behind the network is considered a single broadcast domain, which can have several switches. When a device sends a broadcast packet, the switch sends it to all the connected devices. When this packet reaches the router, it drops the packet. The router routes any traffic with a remote destination address.

A router uses a dynamic routing table, which is updated using the routing protocols. The routers use these routing protocols to listen to their neighbor networks and update their routing tables.

# Access Point

- Is a network device that operates on the Layer 2 or the Data Link layer
- Connects a wireless LAN to the wired LAN – acts like a bridge between the two
- Allows the wireless clients to connect to the wireless LAN, which is identified by a SSID
- Has additional capabilities like a firewall and DHCP server
- Provides a limited range of signals



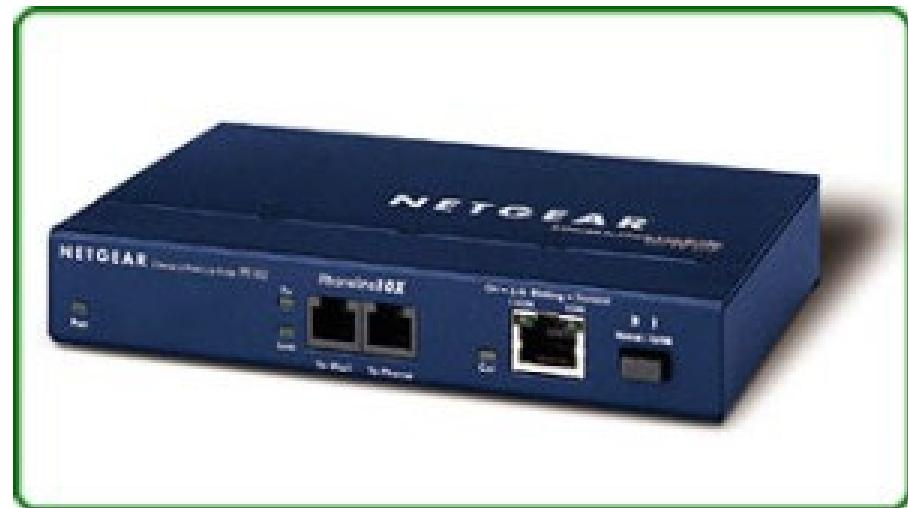
An access point (AP), more commonly known as wireless access point (WAP), is a Layer 2 network device. Layer 2 in the OSI model is the Data Link layer. In a wired network, you may need to create a wireless network. You need to use a wireless access point. It acts as a bridge between the wired and the wireless network. The WAP has one or more Ethernet points that are used to connect to the wired network. Once the WAP is connected to the wired network, it can broadcast the signals to the wireless clients. The wireless network administrator can hide the SSID, which requires the wireless clients to manually enter it on their systems and devices to connect to the wireless network.

Typically, a WAP has several other capabilities other than just providing wireless connectivity. They have capabilities like firewall and DHCP server. They can also include capabilities like guest network and port forwarding. However, all features may not be used all the time. For example, a WAP may have only firewall and DHCP Server enabled in a home scenario, but not the guest network or port forwarding. On the other hand, all these features may be enabled in an enterprise environment.

It is also important to understand that the WAPs have a specific transmission range. If the wireless clients are within this range, they can connect to the WAP. The closer the clients are to the WAP, the better connectivity they get, but the obstacles between the wireless client and the WAP may degrade the wireless signals.

# Bridge

- Is a network device that operates on the Layer 2 or the Data Link layer
- Separates the network into multiple collision domains
- Uses MAC addresses for frame transfers
- Typically has two ports
- Not used in modern networks



jackleahipt.wordpress.com

A bridge is a Layer 2 device that connects two network devices. It can also connect two different networks, such as a wireless network and a wired network. For example, you can connect the wired network to a port on the bridge and connect the wireless router to the second port. The wired network will then be able to route the traffic to the wireless network or vice versa.

Bridges also separate the networks into different collision domains. Each network that connects to it can be a separate collision domain. Unlike a hub, every port on a bridge serves as a collision domain, which eventually reduces the chances of collisions.

Just like a switch, a bridge also works with the MAC addresses. It uses the MAC addresses to send the traffic to its destination. A bridge maintains a bridging table that maintains a list of all known or memorized MAC addresses. These MAC addresses are learned from the packets that arrive at a port on the bridge. For example, if a packet is sent from port 1 to the devices connected on port 2, a bridge may not know where this packet should be sent to. Therefore, the bridge floods the ports looking for the destination MAC address. When a device responds to this request, the bridge maps its MAC address and adds it to the bridge table. Next time, if the packet is meant for the same device, the bridge will find the MAC address in the bridge table and will not have to send out the message to every port.

# Wireless LAN Controller

- Manages the deployed access points in a location
- Is the central authority that controls the existing access points but also prevents the deployment of rogue access points
- Helps in individual access point monitoring
- Has features like interference detection and access point status detection

**Centralized**

**Distributed**



Typically, in an enterprise environment, there will be more than one WAPs installed. If the organization is large and has thousands of mobile users, you need to install several WAPs to ensure the wireless connectivity is provided to them. Individually managing several WAPs can be a time-consuming and difficult task. However, with the deployment of a Wireless LAN Controller, this task becomes easy.

The Wireless Access Controller is deployed centrally to manage each WAP that is installed. It not only manages the WAPs from a centralized location but also keeps track of the WAPs. It prevents any unauthorized WAPs deployment.

Even though several WAPs can be installed, the Wireless LAN Controller enables centralized network management, which helps monitor and manage each WAP. With centralized monitoring, the cost of ownership comes down.

Other than this, there are several features of Wireless Lan Controller:

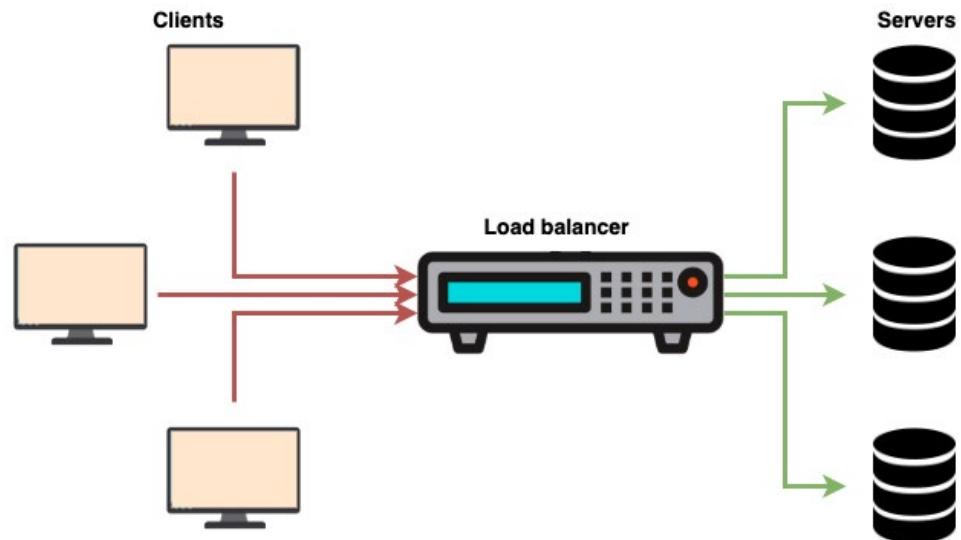
- Easy deployment, management, and maintenance of WAPs
- Simplified wireless network administration
- Interference in the wireless network detection
- WAP status detection

A Wireless LAN Controller can be deployed in two ways:

- Centralized: are installed in a centralized location to manage several WAPs in premises or a building. This model is typically used when the locations where WAPs are in close proximity.
- Distributed: are installed in a small office where the wired and wireless clients are connected to an access switch.

# Load Balancer

- Divide the workload amongst the servers or other network devices
- Helps to achieve optimum utilization of the server resources
- Helps to provide faster response time
- Can be deployed in the form of software and hardware
- Can work with different load balancing algorithms:
- First Come First Served
- Round-Robin
- Weighed Round-Robin
- Is mostly used with Web servers



is.docs.wso2.com

# Load Balancer

A load balancer is an interface to a set of servers to provide a similar service set to the users, who see it as a single server. For example, if you have used any search engines, like google.com, it is not being served by a single server. A load balancer sits in front of several servers that take the request and pass it to the server to return the Web page.

The main role of the load balancer is to distribute the workload amongst several servers. Depending on its configuration, it can look at the server with the minimum workload and pass the request to the server. Alternatively, it can also rotate the requests to servers – one by one. In this manner, no server ever becomes overloaded. Each server has more or less the same workload.

Assume that a Web server is overloaded with the requests. It will take time to serve the requests in this state, which delays the response time. On the other hand, a load balancer distributes the requests amongst the Web servers. The response time is much faster as no server ever becomes overloaded.

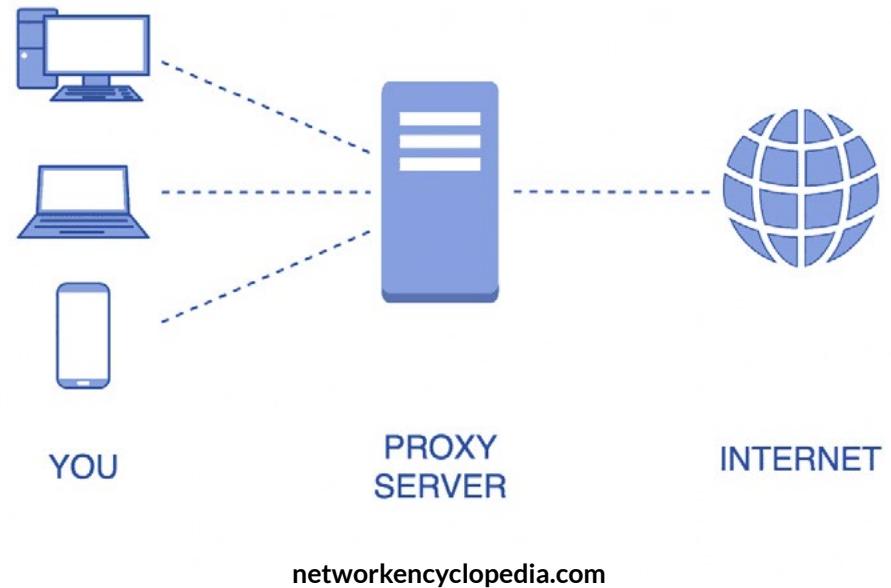
A load balancer can be hardware or software. A hardware load balancer is an appliance that is installed and needs to be managed. In an enterprise environment, it is typically hardware-based load balancers that are used. Software load balancers, on the other hand, are meant for medium-sized traffic. You know that the traffic will not be in a million requests a minute, then you can use the software-based load balancer.

A load balancer can be deployed in three ways:

- First Come First Served: The requests are handled as they arrive. The first request goes to the first server. The second request goes to the second server. Similarly, the requests are sent in a sequence to the additional servers that are configured behind the load balancer. When more requests come, they are not sent to the servers that already have received requests unless they indicate that the previous request has been handled.
- Round-Robin: The requests are handled as they arrive. The first request goes to the first server. The second request goes to the second server. The third request goes to the third server. However, if there are only three servers and when the fourth request comes, it is sent to the first server. In this deployment, a server may receive an additional request when catering to an existing one. Also, a server may sit idle because it finished its first request, but it has to wait for its turn to receive the request.
- Weighed Round-Robin: In this deployment, servers are given weightage. The server with higher weightage receives more requests than the one that has lower weightage.

# Proxy Server

- Is responsible for acting like a middle-man to provide Internet connections to the systems on a network
- Has several capabilities like:
  - Filtering Websites and ports
  - Logging user visits
  - Caching the visited Webpages
- Hides the internal systems to be visible on the Internet
- Requires its IP address to be configured in client's Web browser



# Proxy Server

A proxy server is a server that acts as a middle-man between the clients on a network and the Internet. Its main job is to retrieve the Webpages and serve them back to the clients requested. For example, if a client requests for [www.microsoft.com](http://www.microsoft.com) Webpage, the proxy server will provide the Webpage to the client after it gets it to form the respective Website. In short, it accepts the client's requests and then returns them the Webpages that they had requested.

Besides simply acting as a middle-man to provide the Webpages, it also has several other features, like filtering the Websites and ports. You can configure the proxy server to block certain Websites or certain categories, like gambling. When a user attempts to browse a Website that falls into the gambling Website, the proxy server checks for the Website and either allows or denies access to the user. This way, the filtering of the Websites helps an organization prevent users from visiting unwanted Websites.

Another key feature of the proxy server is to log each user request. The proxy server logs the time, the username of the user who requested the Website, and the date and time. You can analyze the logs to get more insights into the Websites that the users are visiting.

One of the key features of the proxy server is to cache the Webpages that the users request. Let's assume that one of the user requests for [www.microsoft.com](http://www.microsoft.com) Webpage. An hour later, another user requests for the same Webpage. The proxy server checks its cache for this Webpage. If it finds it, it checks whether it has the latest Webpage. If it does, it simply retrieves the Webpage from the cache and returns it to the user. If the cache does not have the latest Webpage, the proxy server first caches the latest copy of the Webpage and provides it to the user. This feature saves time and bandwidth as the same Webpage need not be retrieved by several users. It is downloaded once and provided to the users.

When a user accesses a Webpage via a proxy server, the user's IP address is not visible to the Webserver hosting the Webpage. The Web server only sees the proxy server's IP address. The clients are safeguarded from being visible on the Internet.

For the clients to use a proxy server, their IP address needs to be configured in their Web browser.

# Cable Modem

- Is used to provide Internet connectivity to a system using a cable connection
- Needs to be installed at the location where Internet connection is required
- Is mostly used by home users
- Requires a cable connection to work



[www.pinterest.com/pin/383650461976740269/](http://www.pinterest.com/pin/383650461976740269/)

Other than providing cable services, several cable service providers also provide Internet connectivity to their subscribers. The subscribers need to have a cable modem installed at their locations. The same cable connection is then terminated to the coaxial port. The cable modem also has an Ethernet port, which is used to connect a system.

The home users mostly use cable modems. One of the key reasons is that since the cable television connection is already terminated, it can provide Internet connectivity. Without a cable connection, the cable modem does not work.

# DSL Modem

- Uses a telephone line to provide Internet connectivity
- Receives input from the telephone line and converts it to an Ethernet connection
- Displays the connectivity through various lights
- Sends the Internet traffic to the ISP's router



A DSL modem is used with DSL broadband, which provides Internet connectivity. The DSL broadband is provided using a telephone line terminating into the DSL modem, with one or more Ethernet ports. You can connect a system or a wireless router to this port.

The DSL modem receives the signals from the telephone line and then converts these signals for the Ethernet cable, which further connects a system or a wireless router. The task of converting input from the telephone line or the Ethernet is taken care of by the DSL modem.

There are several indicators on the DSL modem that indicate its status. If the DSL indicator shows green light, you can ensure that the Internet connection is up and working. On the other hand, an orange or red light may suggest that the link is down. Different DSL modem manufacturers label the indicators on the modem differently. You will have to refer to the documentation to understand them.

The DSL modems stay in sync with the digital subscriber line access multiplexer or DSLAM, located at the service provider's premise. When a DSL modem is out of sync, it will not provide Internet connectivity. If it is in sync, it takes the user requests for the Internet and sends them to the routers at the service provider's end.

# Repeater

- Is a Layer 1 device
- Extends the cable beyond its maximum limit
  - Cables have specific length limit after which the signal attenuates
  - Repeaters reproduce the attenuated signals to its original strengths
- Has the capability to amplify the signals
- Usually found in wireless networks



Each Ethernet cable has a certain length to which it can transmit signals. After the length is crossed, the signal starts to attenuate and cannot go beyond the maximum length of the cable. This is where a repeater becomes handy. A repeater is a Layer 1 device that helps you extend the cable length. For example, let's say you have a CAT 5 cable with a limit of 100 meters. It is a known fact that a CAT 5 cable cannot send signals beyond its length. You can install a repeater and extend the CAT 5 cable to go beyond its limit to solve this issue.

Towards the end of the cable, when the signals start to attenuate, a repeater reproduces or regenerates the signals to their original strength. This is done by copying the signal bit by bit and then reproducing or regenerating it to its original strength. However, a repeater cannot amplify the signals for better strength. Repeaters are most often used with the coaxial cables that are used for cable television. Repeaters are also used in a wireless network to extend its signals to a larger area.

# Voice Gateway

- Sends the VoIP traffic over the Internet
- Can connect the Public Switched Telephone Network (PSTN) to the VoIP infrastructure
- Is usually installed at the edge of a network
- Collects the VoIP traffic and sends it to their respective destinations

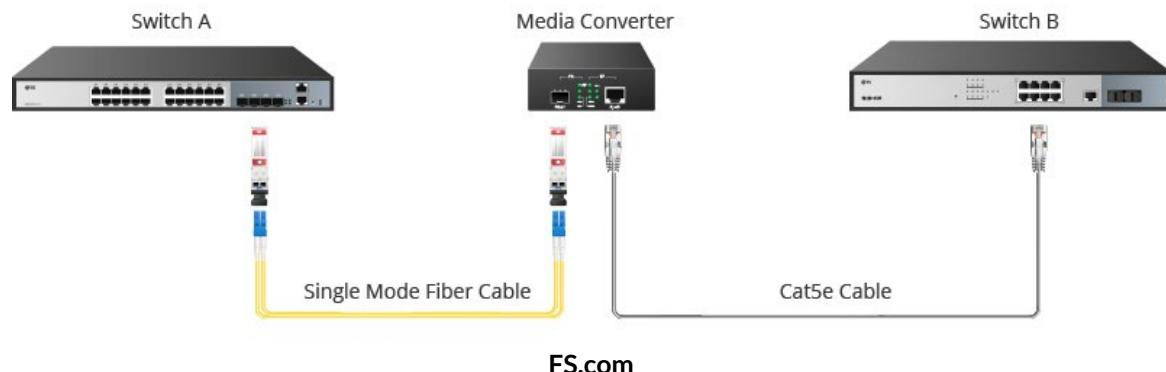


The Voice over IP (VoIP) device sends out the VoIP traffic over the Internet to the service provider. It can also connect the Public Switched Telephone Network or PSTN to the VoIP infrastructure, which can be done with a different type of connectivity, such as T1 or T3 leased lines. The legacy voice devices, such as analog phones and fax machines, use the PSTN network. The conversion of signals from the PSTN network to the VoIP will be performed by the Session Initiation Protocol (SIP) protocol.

An organization may be geographically spread out to different locations. If the organization requires to configure VoIP infrastructure at each of these locations, it would need to install voice gateway at the end of each location's network. For example, if a head office and two branch offices need to be connected via VoIP, then each of these will require a voice gateway.

# Media Converter

- Connects two different media networks
- Works like a transmitter to receive and send signals
- Can be built into high-end switches
- Types:
  - Multimode fiber to Ethernet
  - Fiber to coaxial
  - Singlemode to multimode fiber
  - Singlemode fiber to Ethernet



An organization may have two different segregated networks that were never joined together. For example, one network runs on fiber and the other runs on Ethernet. However, now, the organization needs to join both these networks to form a large network. Now, both the network use different types of cables and cannot be connected. One method is to convert the Ethernet network to the fiber or vice versa. This is a time-consuming task and will create several bottlenecks. Another solution to this problem is to use a media converter, which allows you to connect two different media, such as fiber and Ethernet cables. The media converter has slots for two types of media, such as fiber and Ethernet. When both the cables are connected, the media converter starts working as a transmitter to send and receive signals between different media.

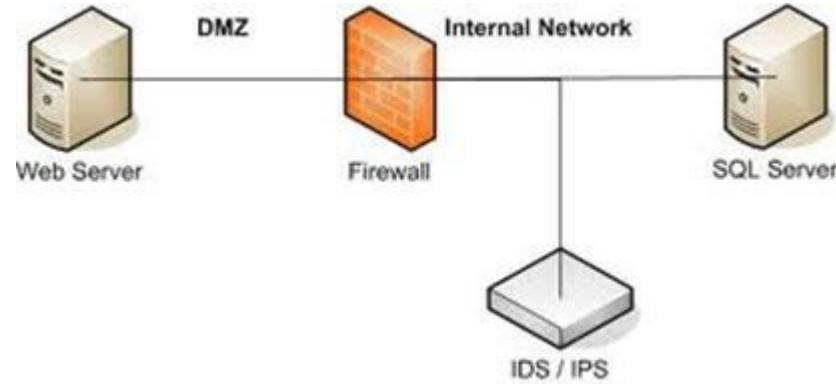
A media converter is a non-intelligent device that does not require any configuration. All you need to do is plug in the different media and rest is taken care of by the media converter. It can be an independent device or built into other devices like switches.

There are different types of media converters available:

- Multimode fiber to Ethernet: Connects an Ethernet network connection over a multimode fiber backbone
- Fiber to coaxial: Converts signals receives from a fiber cable for the coaxial cable
- Singlemode to multimode fiber: Transmits multimode fiber signals over singlemode fiber devices and links
- Singlemode fiber to Ethernet: Connects an Ethernet network to a singlemode fiber backbone.

# IDS/IPS

- Intrusion Detection System (IDS)
  - Monitors the network traffic
  - Contains rules against which the traffic is monitored
  - Sends an alert to the administrator or a logging system if a violation occurs
- Intrusion Prevention System (IPS)
  - Monitors the network traffic like IDS but also blocks the traffic
  - Performs real-time monitoring
  - Can take actions like dropping the traffic



[www.smallnetbuilder.com](http://www.smallnetbuilder.com)

On a network, much traffic is transmitted. No one can know whether the traffic is legitimate or malicious. Even if you can detect malicious traffic, handling it becomes another problem.

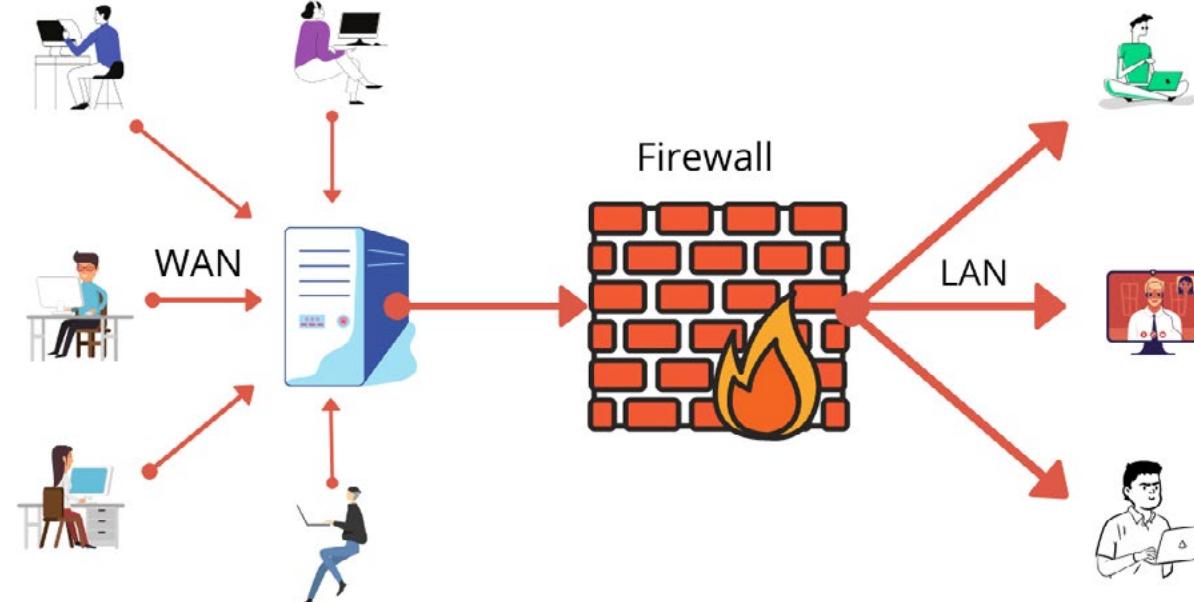
To tackle this problem, you need to install an Intrusion Detection System (IDS), which helps you monitor the network traffic. An IDS works with the rules that can be configured to monitor the traffic. If the traffic violates any rules, then it is malicious traffic. As soon as the IDS detects any traffic that does not match its rules, it alerts the administrator. It can also be configured to send alerts to centralized systems like Security information and event management (SIEM). An IDS cannot perform any other tasks beyond detecting and logging the malicious traffic.

An intrusion prevention system (IPS) performs the detection just like an IDS, but it does much more than just detecting the traffic. It can also block or drop malicious traffic. One of the key features of an IPS is that it performs real-time monitoring and can perform various actions once the malicious traffic is detected. For example, it can drop malicious packets. It can even be configured to shut down the port on which the malicious traffic is flowing through.

Both IDS and IPS are available for host and network. The host-based IDS is called host IDS or HIDS. The network-based IDS is called network IDS or NIDS. Similarly, the host-based IPS is called host IPS or HIPS. The network-based IPS is called network IPS or NIPS.

# Firewall

- Is meant to monitor and filter the incoming and outgoing traffic
- Prevents the unauthorized traffic from entering the network
- Is installed on the edge of a network
- Can be categorized as:
- Hardware-based
- Software-based
- Can be of two types:
- Host-based
- Network-based



geekflare.com

# Firewall

A firewall is like a network gatekeeper as it is located on the edge of a network. Without a firewall, a host or the network is exposed to the Internet. Any application, ports, or even services are exposed to external entities, which can be malicious enough to take their advantage by exploiting them. It monitors and filters the incoming and outgoing traffic from a network based on the rules. When installing a firewall, you need to configure it with the security rules, which can either allow or drop the traffic. For example, if you have configured the firewall to block FTP, if any user attempts to connect to an FTP server out of the network, the traffic is blocked and dropped by the firewall.

Similarly, if a rule is configured to allow only HTTPS traffic and deny every other kind of traffic, the firewall will allow the users to connect to services that use the HTTPS protocol. Even HTTP protocol traffic will be dropped. You can even configure a rule to allow the traffic to a specific IP address or the host. For example, you can configure the traffic on the SSH port for a specific host from your network. If users attempt to initiate an SSH connection to any other host, then they are denied access. However, if the users attempt to connect to the host mentioned in the allow rule, users will be able to establish the connection.

You can categorize the firewalls into two categories:

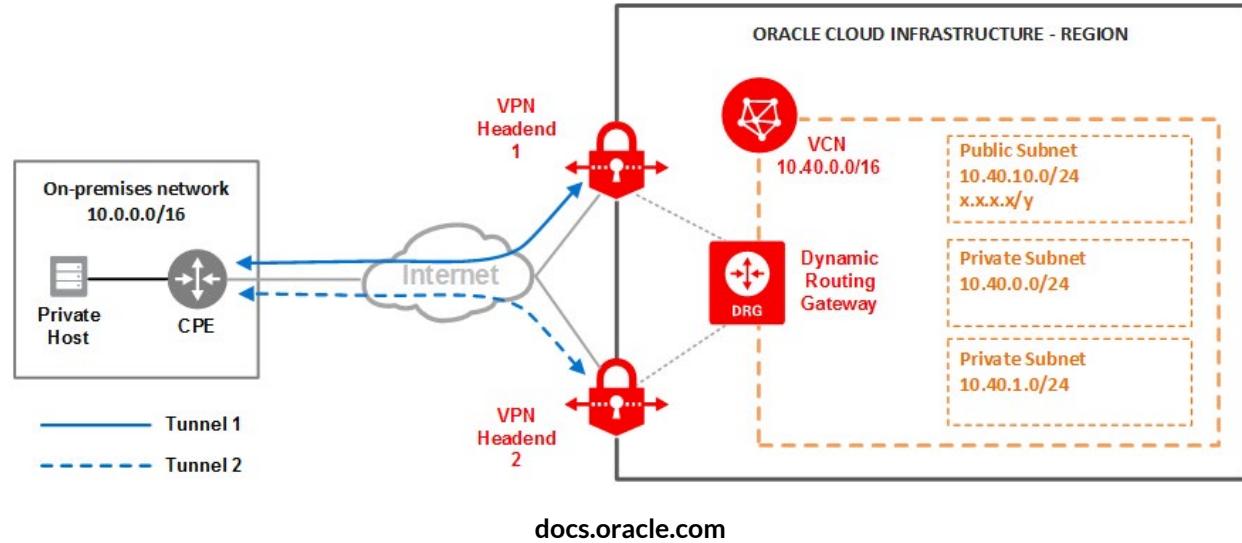
- Software-based: These applications can either be standalone or part of another application or the operating system. For example, ZoneAlarm is an independent firewall application that is installed on an operating system like Windows. Windows Defender Firewall is part of the Windows operating system. BitDefender Total Security, which is an antimalware package, also has a firewall module.
- Hardware-based: These are hardware appliances that act as a dedicated firewall. These appliances are installed on the edge of the network. An example of such an appliance is Cisco Adaptive Security Appliance (ASA).

A firewall can be a host-based firewall, which can detect only the local system. Windows Defender Firewall is one such example. The second type of firewall is network-based, usually a hardware-based firewall like Cisco Adaptive Security Appliance.



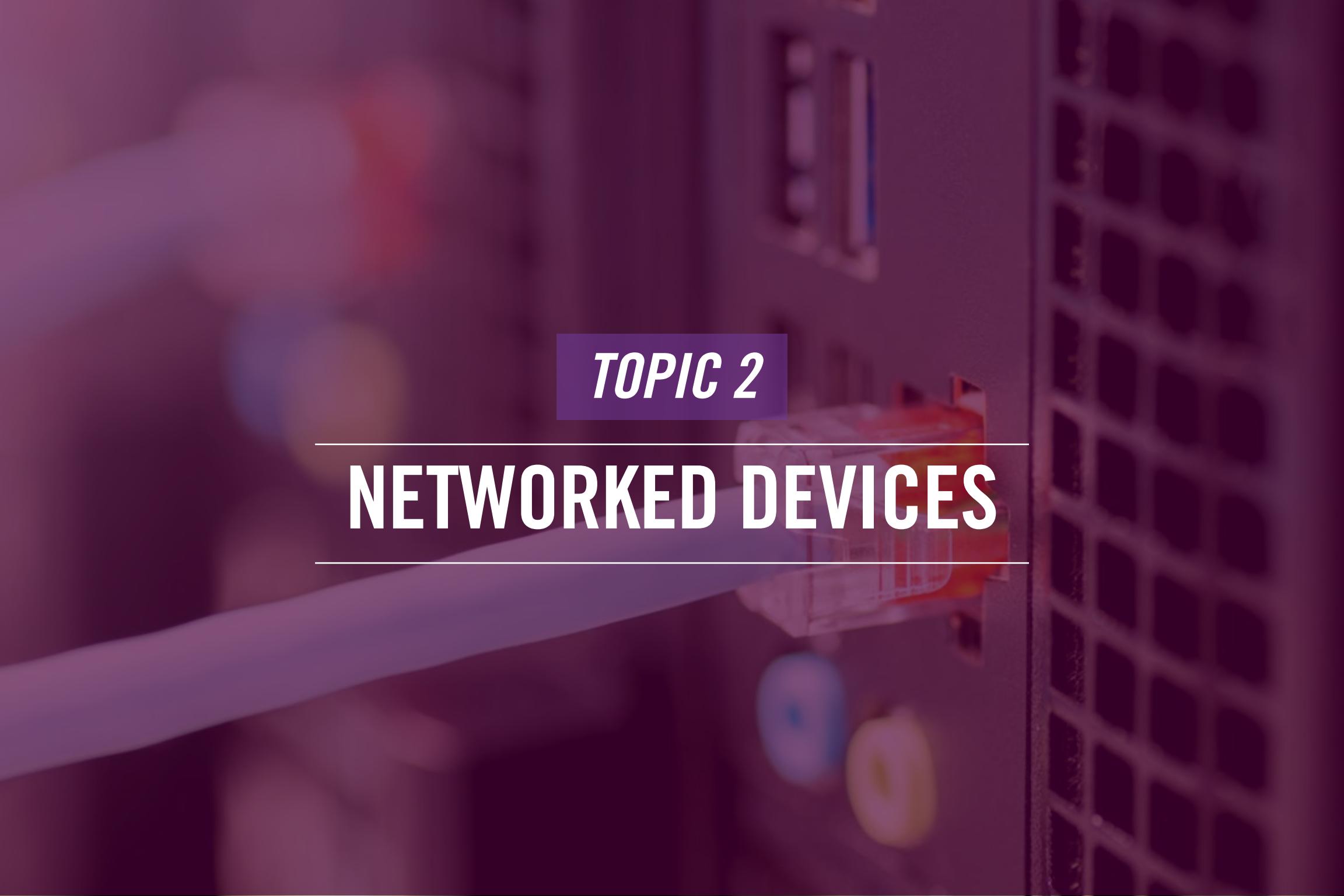
# VPN Headend

- Is the terminating point of a VPN tunnel
- Can support route-based or policy-based tunnels
- Are typically deployed in pair for redundancy
- Supports a single encryption domain



A VPN headend is a device used to terminate the VPN connections at the service provider's end. An organization connects with a service provider using a VPN tunnel that needs to be terminated. The VPN headend device is the terminating point at the service provider's end. The main function of the VPN headend is to receive the signals, decode, and send them forward. For the outgoing traffic, it has to encode and sent it forward.

It can be configured with route-based or policy-based tunnels. In most cases, the VPN headend is deployed in pairs for redundancy. The VPN headend provides support for only one encryption domain. If there are multiple encryption domains in the configuration, such as the policy, it will not work.



*TOPIC 2*

---

# NETWORKED DEVICES

---

# Voice over Internet Protocol (VoIP) Phone

- Uses the VoIP infrastructure to make or receive calls
- Converts the sound to digital packets
- Sends them to the recipient
- Converts the digital packets back to sound at the recipient end
- Uses the Session Initiation Protocol (SIP) for initiating, establishing, and terminating the connection
- Can be of two types:
- Hardware-based
- Software-based
- Cloud-based



Like analog phones are used with the PSTN infrastructure, a VoIP phone uses the IP infrastructure to send and receive calls. When a call is made using a VoIP phone, it converts the sounds to digital signals transmitted through the IP infrastructure to the recipient. The recipient at the receiving end must also have the VoIP phone, which then converts the received data packets back to the sound. The Session Initiation Protocol (SIP) is used for initiating, establishing, and terminating the connection.

VoIP phones can be of two types:

**Hardware-based:** These are the physical phones used to receive and make calls through the VoIP network. They are similar to analog phones but have many more features but do not work with the PSTN lines. Hardware phones can be different types, such as desk, USB, wireless, or conference phones.

**Software-based:** These are applications installed on the system and use the system resources like the sound card and microphone. Other than the system, you also have mobile apps that work as VoIP phones.

Some VoIP phones operate in the cloud and do not require a PBX. Cloud-based VoIP phones do not function with analog phone lines.

# Printer

- Is a print device that is used for printing documents
- Can be of different types:
  - Inkjet
  - Dot-matrix
  - Laser
  - 3D
  - LED
- Can be connected via:
  - USB cable
  - Over the network
  - Wireless



[in.pcmag.com](http://in.pcmag.com)

# Printer

A printer is a hardware device that prints documents. Most of the operating systems, like Windows, have printer drivers for several types of printers. When you connect a printer to a system, the printer is detected and installed automatically if the drivers are available within the operating system. If drivers are not available within the operating system, you need to download the drivers and install them.

There can be different types of printers, such as:

- Laser
- Inkjet
- Dot-matrix
- 3D
- LED

You may have a question as to which one to use. The answer is that it depends on the requirements. For example, if you need to print bills at a cash register, the dot-matrix printer is probably the best option. Similarly, when you have many documents to be printed, such as in an office environment, then a laser printer is best suited.

A printer can be accessed via different mediums. The majority of the printers have a USB port that can connect a printer to a system. With this kind of configuration, the printer is accessible only to the system. However, a user can decide to share the printer. The other method is to configure the printer with an IP address on a network. In most organizations, printers are configured on the network and then shared. The third type is wireless printers. Nowadays, several printers come with wireless capabilities. You can connect it to a wireless network, but you can also use the hotspot built into the printer.



# Physical Access Control Devices

- Are hardware devices that allow or deny entry to a specific room or location
- Are configured with rules to allow or deny entries
- Can be of different types:
- Digital locks
- Card readers
- Biometric devices
- Encrypted badges
- Fobs
- Can be coupled as a multi-factor authentication



[www.integratedaccesssecurity.com](http://www.integratedaccesssecurity.com)

Physical access control devices are hardware devices that allow or deny entries based on a rule or condition. Let's take an example of an organization where no one is allowed to enter the premises after 6 PM until 6 AM the next morning. The entrance of the premises has a badge reader that checks for the entry time. If it is 6 PM or later, the user is denied entry. Any other time from 6 AM to 6 PM, the users are allowed entry into the premises.

Some of the key physical access control devices are:

- Digital locks
- Card readers
- Biometric devices
- Encrypted badges
- Fobs

You can also use the physical access devices as part of the multi-factor authentication. For example, one method can be the badge reader, and another can be the digital lock or biometric device for fingerprint scanning.

# Cameras

- Are used for surveillance purposes
- Can be deployed inside and outside a facility
- Can capture image or record videos
- Can be of different types:
  - Fixed
  - Pan-Tilt-Zoom (PTZ)
  - CCTV
  - IP-based



Cameras are mainly used for either clicking pictures or recording videos. However, in the IT world, cameras are mainly used for surveillance purposes. When you visit a coffee shop or a departmental store, you would have seen signs that say, "You are under CCTV surveillance". This means that there are closed-circuit television (CCTV) cameras installed to record the location and the movement of people. CCTV cameras are connected with a system that performs recordings and saves them.

You can deploy different types of cameras depending on your need:

- Fixed: Are fixed in a specific location to record the individual's movements as they pass through a specific location.
- Pan-Tilt-Zoom (PTZ): Can zoom on to a specific individual in a crowded location.
- CCTV: Are used for recording the footage of a specific location, such as an entry gate or a passage.
- IP-based: Are Ethernet-based cameras that are connected to the network using a cable. These cameras are assigned IP addresses for monitoring purposes.

They can be Power over Ethernet (PoE)-based cameras that do not require any power source and get the power from the Ethernet cable.

# HVAC Sensors

- Are a key component in the Heating, Ventilation and Air Conditioning (HVAC systems)
- Help you detect:
  - Excessive heat
  - High or low humidity
  - Rising temperature
- Can be of different types, such as:
  - Pressure
  - Temperature
  - Humidity



[www.galltec-mela.de](http://www.galltec-mela.de)

# HVAC Sensors

HVAC stands for heating, ventilation and air conditioning. When you construct a building, you need to be conscious of HVAC. HVAC systems are designed to use sensors to manage and increase efficiency in managing HVAC. Some of the key components of HVAC systems are:

- Sensors
- Controllers
- Output devices
- Communication protocols
- Terminal interface

Each component is controlled either by firmware or software. Even though each component is critical, sensors play a vital role in HVAC systems. They are responsible for identifying equipment malfunctions or improper conditions that can lead to environmental hazards. For example, sensors can detect:

- When there is an excessive heat
- When there is high or low humidity
- When the temperature shoots up

## 1. Pressure Sensors

Pressure sensors monitor pressure levels within specific zones, and measure the pressure drop across filters and other devices, effectively alerting the system when maintenance and filter replacement is required. Accurate pressure measurement is vital for optimal HVAC system performance. Pressure sensors can measure extremely high and low pressures in air and water applications offering precise measurement of pressure, differential pressure, and velocity for reliable monitoring.

## 2. Temperature Sensors

Temperature sensors measure air and water temperature and adjust the heating and air conditioning to raise or lower the air temperature based on the programmed setpoint preventing wasted energy. You can also use the sensors' data to learn about a room's airflow and air quality.

## 3. Humidity Sensors

Controlling humidity in buildings is critical for occupant comfort, safety and protecting building infrastructure, production processes, stored goods, and museum artwork. Combined temperature and humidity sensors provide a flexible and cost-effective solution. Humidity control typically adds clean steam to the airstream to raise space humidity.



# Internet of Things (IoT) Devices

- Are hardware devices that have an IP address to communicate over the Internet or a network
- Have various components, such as
  - Software
  - Sensors
  - Actuators
  - Network connectivity
- Can be communicated and controlled via the Internet
- Send data to a centralized server
- Can be refrigerator, smart speakers, smart thermostats, smart doorbells, and watches



HVAC acronym denotes heating, ventilation and air conditioning. These are critical components when designing and constructing a building. These components can be managed using sensors that are deployed strategically in a building. For example, such sensors are typically deployed in a data center to monitor excessive heat, humidity, and temperature.

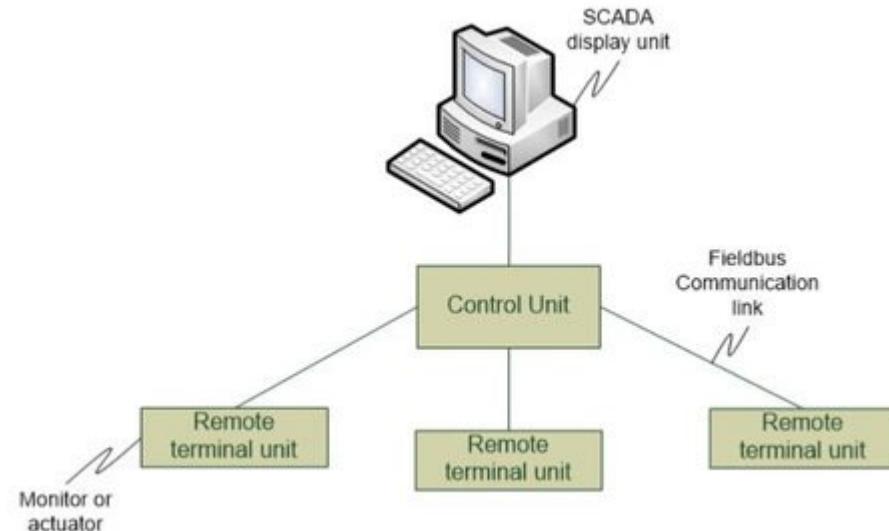
When sensors are deployed, they can monitor the temperatures of individual equipment and raise alarms for malfunctions or improper conditions that can be dangerous for the surrounding equipment and environment. For example, excessive heat may lead to the burning of cables. Sensors can help raise timely alarms to prevent any such mishap.

Even though there are several types of sensors, but some of the key sensors that are typically used are:

- Pressure Sensors: Used to measure the pressure levels and raise alarms if the pressure is nearing the threshold levels. One such example is measuring air pressure.
- Temperature Sensors: Used for temperature measurement. The air conditioning temperature can be adjusted to avoid any equipment damage with timely alarms or alerts.
- Humidity Sensors: Help you measure the humidity of a specific place. Humidity can cause faster corrosion and internal damage to the system components. Sensors can raise alerts if the humidity goes beyond a specific threshold.

# ICS/SCADA

- Industrial Control System (ICS)
  - Is a type of command-and-control system used in industrial plants
- Supervisory Control and Data Acquisition (SCADA)
  - Manages the ICS systems and provides complete control over the running processes and allows them to be changed in real-time
- Comprises of several components:
  - Master Terminal Unit (MTU)
  - Remote Terminal Unit (RTU)
  - Human Machine Interface (HMI)



[www.kuppingercole.com](http://www.kuppingercole.com)

An Industrial Control System (ICS) is a set of mission control systems and applications used to monitor the processes in industrial plants. The ICS applications are managed by the Supervisory Control and Data Acquisition (SCADA) systems that use a graphical user interface (GUI) to display a dashboard that provides insights into the ICS systems and applications by displaying their current status. With the use of SCADA, you can manage the ICS systems and control the running processes in real-time. For example, if you need to tweak the parameters of a conveyor belt to run it at a different speed, you can do it in real-time. With SCADA, you get a complete view of the running processes and the control to manage them. The running systems generate data, which can be collected, monitored, and stored via the SCADA systems.

SCADA has several key components:

- Master Terminal Unit (MTU): Collects the data from Remote Terminal Units (RTUs).
- Remote Terminal Unit (RTU): Connect with the devices monitored via sensors and collect data to share it with MTUs.
- Human Machine Interface (HMI): Displays the data in a dashboard format.

# Summary

- Networking Devices
- Networkeda Devices



That's the end of the lesson.

Here we covered :

- Networking Devices
- Networked Devices





*NEXT TOPIC*

---

# ROUTING AND BANDWIDTH MANAGEMENT

---

Lesson

2

---

# Routing and **Bandwidth Management**

- 1 — Welcome to the lesson 2 of Module 2. In this lesson, you will learn about the:
  - 2 — Routing and Bandwidth Management
- 



Network Fundamentals

# AGENDA

- Routing
- Bandwidth Management



Hi, welcome to COMPTIA Network+ Course  
In this lesson we will talk about:

- Routing
- Bandwidth Management



*TOPIC 1*

---

# ROUTING

---

# Routing and Its Types

- Works on Layer 3 of the OSI model
- Is performed by a router
- Is a method of sending data to a destination network by using its network address
- Uses routing tables to make a decision
- Works in three different modes:

Static

Dynamic

Default

Have you ever imagined how you can open [www.google.com](http://www.google.com) in a Web browser or watch a video on [www.youtube.com](http://www.youtube.com)? How does your computer reach these respective websites? Your system does not know where these websites are? This is the job of the router to find these websites for you. Overall, it is not very easy, but in a nutshell, a router is an entity that finds the paths for you to reach these websites. These paths are known as routes.

Routes are used in routing, which moves the data from the source to the destination device. Routing occurs on Layer 3, the Network Layer, of the OSI model. A router is responsible for performing routing based on the network address in an IP address.

A router uses a routing table to make its routing decisions. In most cases, the routes are dynamically entered in the routing table. However, you can also enter them manually. The router decides to move packets from the source to the destination network based on the routing table. The router checks for the header of each packet that it receives. The header contains the destination address. After getting the destination address, the router determines the route based on the information contained in the routing table.

There are three types of routing:

- Static
- Dynamic
- Default

Let's move ahead to learn about each one of them.



# Static Routing

Default

Dynamic

Static

- Is used in smaller networks that do not require any architectural changes
- Works best with one or two routers
- Requires routing tables to be manually updated
- Can be error-prone
- Requires the use of -p parameter to make the route persistent

In static routing, the routing table is maintained and updated manually. Static routing is typically used in smaller networks that have fewer systems and destinations. Smaller networks usually have one or two routers that can be statically configured with the routing information.

When a route is manually added into the routing table using the route command, it is not a persistent route. When the router reboots, the static route will be removed. Even after the router reboot, this router will remain in the routing table. You can use the -p parameter with the route command to resolve this issue to make it a persistent route.

However, manually updating the static routing tables causes administrative overheads. Every time there is a route change, you have to update the routing table manually. You need to add the static entry. This method is not only time-consuming but also error-prone.



# Dynamic Routing

Default

Dynamic

Static

- Uses the routing protocols that communicate with the network devices
- Routers learn the routes from neighboring routers
- A routing table can contain multiple routes to a single destination
- Routes in the routing table are adjusted automatically
- Requires no manual intervention in updating the routing table
- Requires the use of same routing protocol if two routers need to exchange the routing information

Dynamic routing is used in large networks where it is not possible to maintain multiple routers manually. Several routing protocols can be used to update the routing tables dynamically. Two examples are Routing Information Protocol (RIP) and Open Shortest Path First (OSPF). In the next few slides, you will learn about these protocols.

Unlike static routing, dynamic routing does not require any manual intervention. The routers connect with the neighboring routers to learn about them. Different routers may suggest different routes to a single destination. Therefore, a routing table may contain several different routes even to a single destination. Depending on the protocol you use, the best path may be selected to send the information to the destination host.

As the name suggests, in dynamic routing, the routing table is updated automatically. Even though no manual intervention is required, you can still add a static route if needed.

One of the benefits of using dynamic routing is that it automatically adjusts the routes based on their state. It can send the traffic based on the best possible route. If one of the routes goes down, the routing table is updated to send the traffic through another best possible route.

Dynamic routing requires both routers, one on each end, to use the same routing protocol to exchange the routing information. Because there is a constant exchange of routing information between the routers, more bandwidth is consumed.



# Static Routing

## Default

- Forwards all packets to all destinations through a single router
- Uses the single router as the default gateway
- Uses the stub router, which is the single router receiving packets for all destinations
- Is mainly used in smaller networks where a single router is the entry or exit point

## Dynamic

## Static

Default routing exists in networks that have a single router. All packets that are headed outside the local network are forwarded through a single router. When a packet arrives at the router, it checks for the destination address. If it is not on the local network, the router forwards the packet to the next hop using the default route. In such a scenario, a default route is a route on which the traffic is forwarded because no alternate route is available.

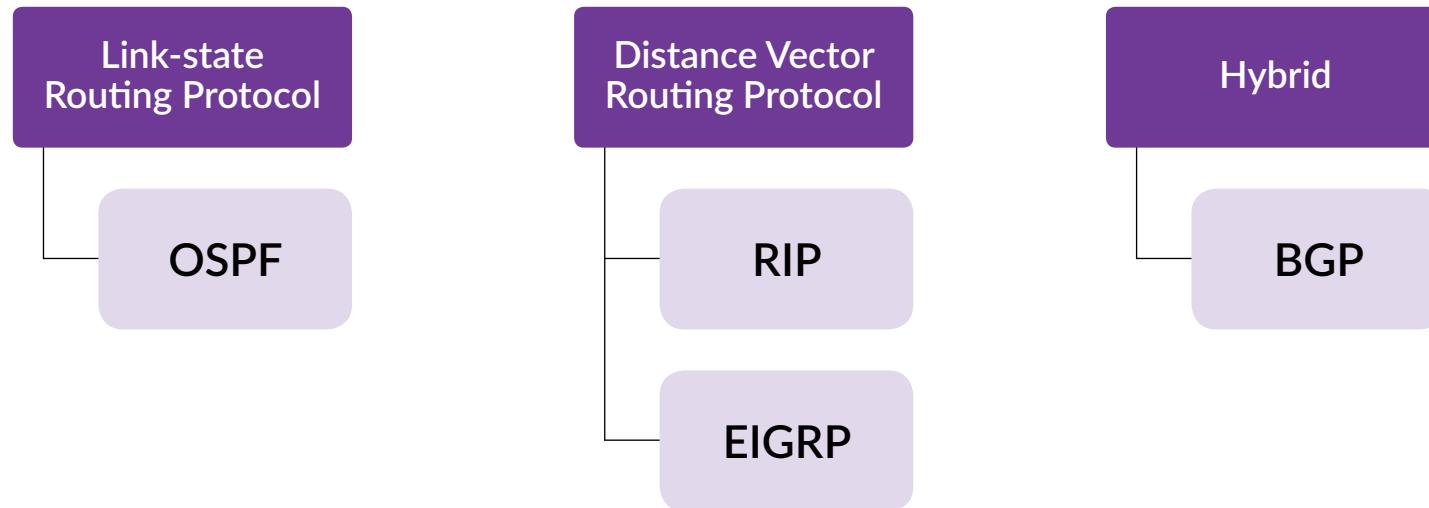
The single router acts as the gateway for the internal traffic to go out of the network. No matter what the destination is, the default route is used for sending out the traffic. The default route can exist in both IPv4 and IPv6 networks.

- IPv4: 0.0.0.0/0 or 0/0
- IPv6: ::/0

You can take the example of an organization that has Internet connectivity from a service provider. The organization's router usually has the default route to the service provider. It will forward all external bound traffic through the default route. When you are using dynamic routing, a default route is created as a static entry. This default route is the gateway of the service provider. Any traffic that is intended whose destination is not known is sent through the default route.



# Dynamic Routing Protocols



Routing protocols are broadly categorized into three different categories, link-state, distance vector, and hybrid. In the next few slides, you will learn about these routing protocols.

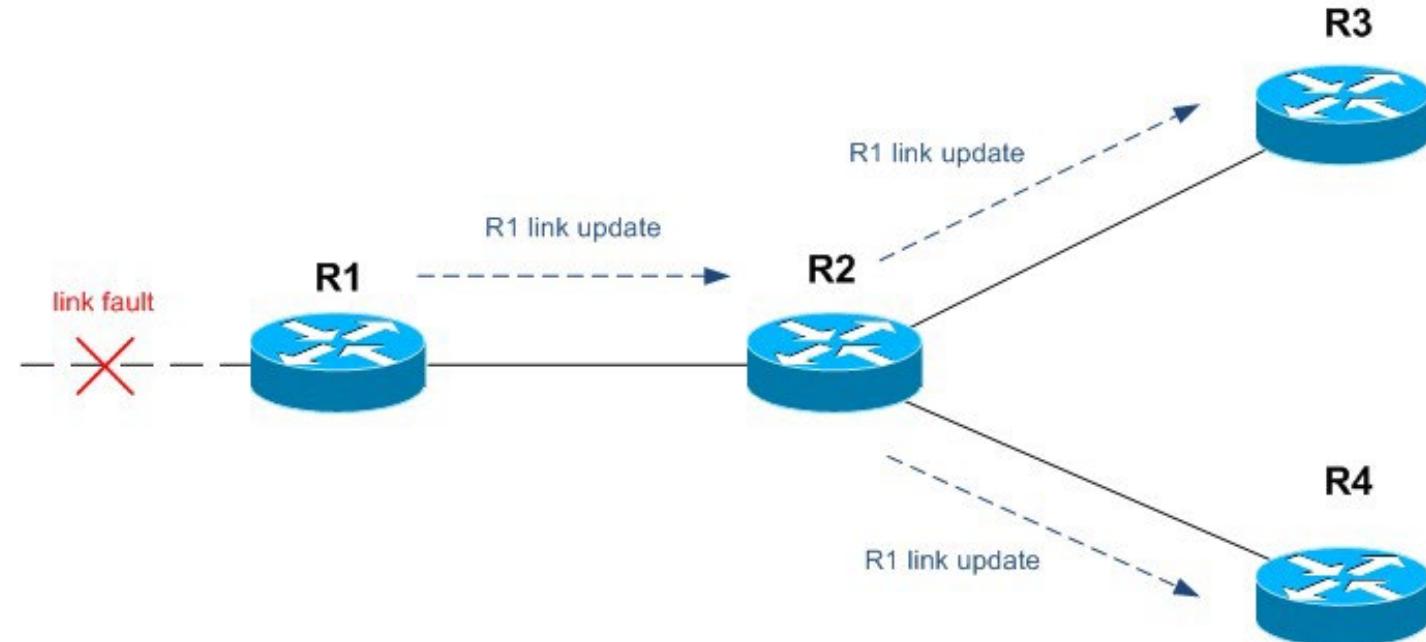
# Link State

Hybrid

Distance Vector

Link State

- Build an entire network map by collecting information from directly connected routers
  - Uses it to select the best path to destination
  - Forwards the updates on the network changes to the neighboring routers
- Calculate the best path based on the least cost, speed, and link congestion
- Sends updates when there are triggered updates



# Link State

A Link State routing protocol builds an entire network map by collecting the information from the directly connected routers. The Link State routing protocols are good in their work as they have the complete network map because they can get first-hand information from the routers they are in touch with.

The Link State protocol works in a simple manner. A router using this protocol contains the following information:

Its own information

Connected links and their status

Each router using the Link State protocol shares the complete information with the other routers. In this way, the information is passed from router to router. Each router has complete information about the neighbors and the connected links. So, therefore, each router has identical information, which can be used to make the routing decisions.

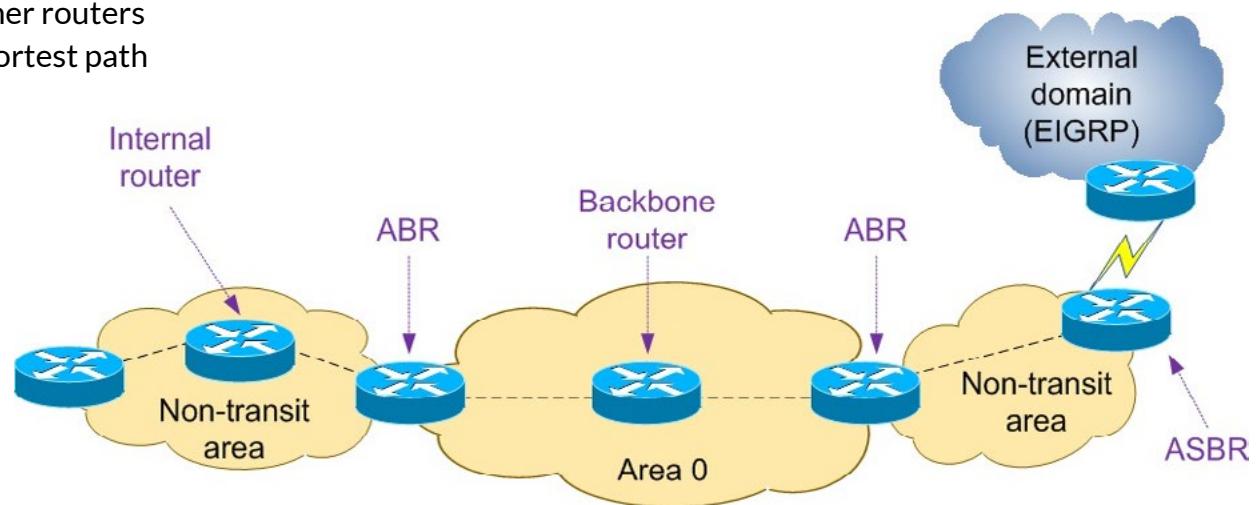
When a router needs to send out the information, the Link State protocol has to decide which route is the best. There is always the possibility of having multiple routes to a single destination. The Link State protocol makes the decision based on the following factors:

- Speed
- Link cost
- The current state of the link - congestion

The routers using the Link State protocol do not broadcast their routing tables. They only send updates whenever there is a change in their routing table.

# Link-state Routing Protocol - OSPF

- Uses the shortest-path algorithm to find the shortest path to the destination
- Calculates the path based on the cost of the route
- Determines the network design by publishing its list of neighbors
  - Routers share a list of neighbors with the other routers
  - This information is used to determine the shortest path



Open Shortest Path First (OSPF) is a Link State routing protocol. When routers are configured with OSPF, they work with the Shortest Path First (SPF) algorithm to find the least-cost path. This method is used every time the traffic needs to be sent to a destination. The routers share the list of the neighboring routers to the other routers, which can then find the shortest path to the destination.

Each route has a cost attached to it. The shortest path is then calculated based on the cost, which is calculated using the link-cost parameters.

Along with the map of the network destinations. As a Link State protocol, each router using the OSPF keeps a link state database. Each router has the same set of information, but they are independent when calculating the cost of a route to reach a particular destination. Therefore, it can be a possibility that two routers may use different routes to reach the same destination.

The backbone of the OSPF network is known as Area 0. Each area you create must be connected to Area 0, which is the backbone of the OSPF network. However, you can create more areas and assigned them numbers like Area 10.

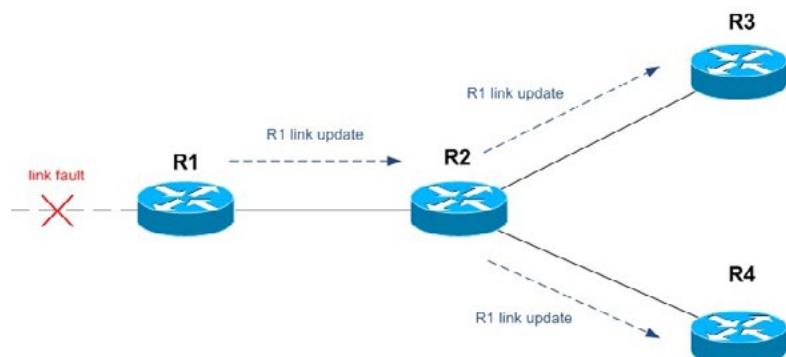
# Distance Vector

Hybrid

Distance  
Vector

Link State

- Uses hop count for path calculation
  - Each router on the way is a hop
  - Router communicates only to the neighboring routers
- Does not require the router to know the complete network path
- Performs frequent updates
- Examples:
  - Enhanced Interior Gateway Routing Protocol (EIGRP)
  - Routing Information Protocol (RIP and RIPv2)



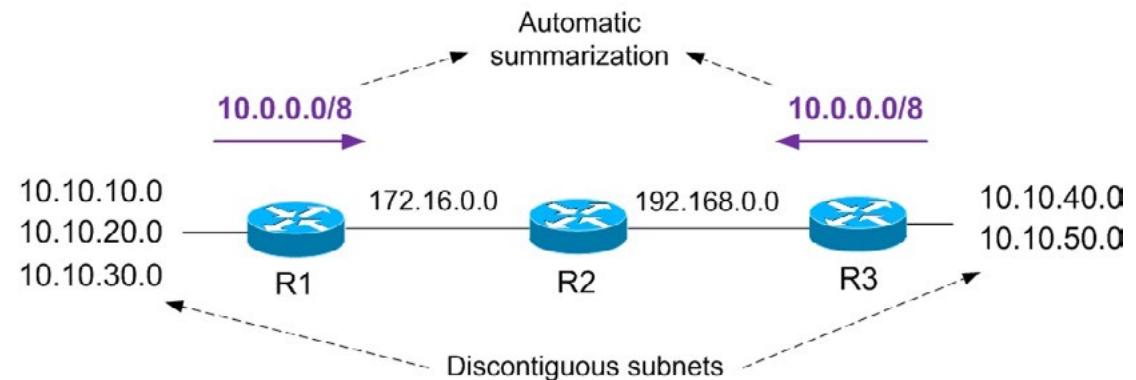
Unlike the Link State protocol, which uses the shortest path as the metric, the distance vector protocols use the hop count. When you have several routers in the distance vector network, each router is considered a hop. The distance vector protocols do not know about the complete network but only their own immediate neighbors. These are the neighbors that a router communicates with.

Because of its lack of knowledge of the entire network, a router is limited to communicate with the neighbors. The router shares its routing table with the immediate neighbors and continues to send periodic updates. Whether changes occur in its routing table, the router still keeps sending the update to the neighbors. The router can also update its routing table based on the information received from the neighbor routers.

Two examples of a distance vector protocol are RIP and IGRP.

# Distance Vector Protocol - RIP

- Is a Distance-vector routing protocol
- Was used for dynamic routing in smaller networks
- Sends the complete routing table to the next router
  - Every 30 seconds
- Has a maximum hop count of 15
  - Anything beyond 15 hops is unreachable
- Has three versions:
  - RIP version 1: Uses broadcast
  - RIP version 2: Uses multicast
  - RIP Next Generation: Works with IPv6



The Routing Information Protocol (RIP) is a distance-vector protocol that can perform dynamic routing. Mostly, RIP is used in smaller networks. RIP also maintains a routing protocol that it shares with its neighboring routers like the other routing protocols. The complete routing table is shared every 30 seconds whether or not it has been updated. As it is a distance vector routing protocol, it uses the hop count metric.

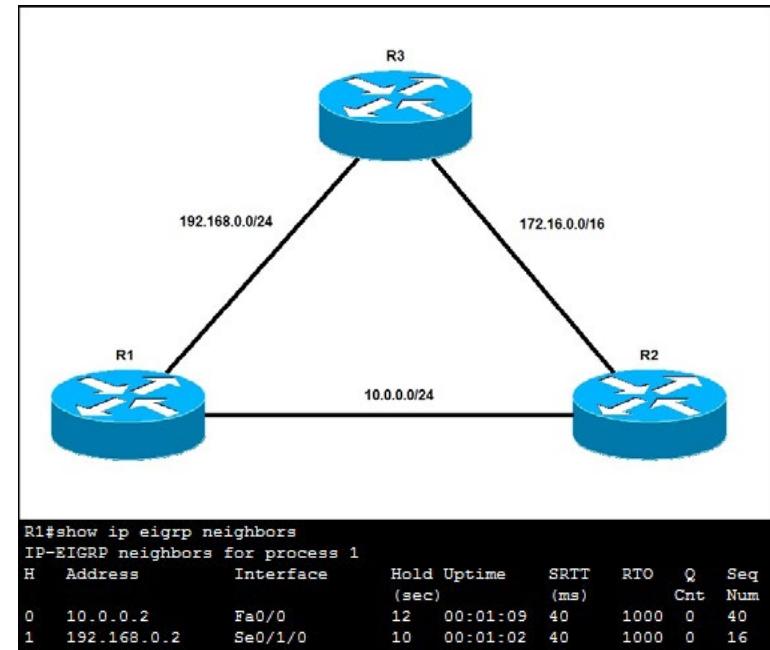
RIP, as stated earlier, is used in smaller networks. One of the biggest reasons is its limit of 15 hops. RIP cannot extend beyond the 15th hop. Anything beyond 15th hop is considered unreachable.

There are three versions of RIP:

- RIP version 1: Sends out the routing table updates using broadcasts. It works with classful routing.
- RIP version 2: Sends out the routing updates using a fixed multicast address, which is 224.0.0.9. It works with classless routing.
- RIP next generation(RIPng): Sends out updates in an IPv6 implementation. It also uses an IPv6 multicast address, which is FF02::9. The multicast address is used to transmit route updates and the routing table after every 30 seconds.

# Distance Vector - EIGRP

- Is an advanced Distance-vector routing protocol
- Performs efficient routing information exchange
- Keeps a copy of the neighbor's routing table to find the best route
- Performs unequal path load-balancing
- Stores the following information on each participating router:
  - Neighbor table – stores the neighbor's information
  - Topology table – stores the neighbor's routing information
  - Routing table – stores the best routes to the destination networks



[EIGRP tables | CCNA# \(geek-university.com\)](#)

EIGRP stands for Enhanced Interior Gateway Routing Protocol. The EIGRP routers contain the neighboring routers' routing information and use it to find the best route to the destination. It can check the stored information of the neighboring routers and decide the best possible route. This eventually leads to efficient routing because the routers do not have to send out queries for the best possible route.

An EIGRP router contains the following information about the neighboring routers:

- Neighbor table – stores information on the neighboring routers. The information includes the neighboring router's IP address hold-down timer and the round-trip timing.
- Topology table – stores routing information of the neighboring routers' routing tables, which contains the metrics for the EIGRP routes.
- Routing table – stores the information about the destination network.

# Hybrid

## Hybrid

## Distance Vector

## Link State

- Is a combination of distance vector and link-state protocols
- Uses TCP for communication between the routers on the Internet
- Provides support for Autonomous System Numbers (ASNs)
- Uses routing table to:
  - Know the list of routers and their reachable destinations
  - Their cost metrics for each path

A hybrid protocol is a combination of distance vector and link state protocols. Border Gateway Protocol (BGP) is an example of a hybrid protocol that uses TCP to communicate with routers on the Internet. BGP uses Autonomous System Numbers (ASNs), globally unique numbers assigned to the IP networks.

Just like any other routing protocol, BGP also uses the routing table for:

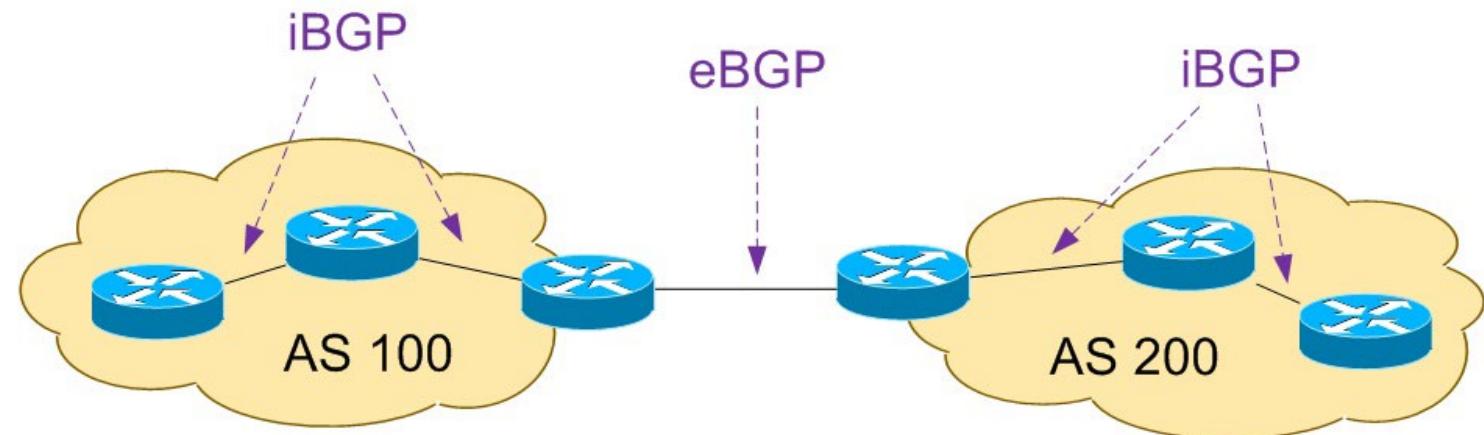
- list of known routers
- the destinations that these routers can reach
- a cost metric for each path leading each router

Based on the available information, it can find the best path or route to the destination to choose the best available route. BGP communicates between the routers using TCP.



# Hybrid - BGP

- Is an inter-autonomous domain communication protocol
- Is an application-layer protocol that works on TCP port 179
- Uses the following for communication:
  - Internal BGP (iBGP): Within a single autonomous domain
  - External BGP: Between multiple autonomous domains
- Can work with:
  - Single-homed
  - Dual-homed sites
  - Multi-homing
  - Dual multi-homing



# Hybrid - BGP

Border Gateway Protocol, most commonly known as BGP, is a hybrid routing protocol. It can perform inter-autonomous domain communication using the TCP port 179. BGP can work in two different ways. It can be:

Internal BGP (iBGP): Within a single autonomous domain. Communication is restricted only within the single autonomous domain. It works like the OSPF protocol.

External BGP (eBGP): Between multiple autonomous domains. Several autonomous domains communicate with each other using eBGP.

Because of its capabilities to use eBGP, BGP can communicate with several autonomous domains on a large network like the Internet. Another capability of BGP is that it advertises its routes and learns the routes from the other routers to choose the best route to reach the destination. In most cases, the Internet Service Providers (ISPs) use BGP to learn and provide routing information.

Because of its capability to work within and with multiple autonomous domains, BGP can work in different ways. Let's look at them.

- Single-Homed: A single-homed site uses a single ISP connection. It advertises its routes with the ISP and learns its default route.
- Dual-Homed: Instead of one single connection, there are two connections from the single ISP. These connections can be configured on a single router or two routers, mainly used for load balancing.
- Multi-Homed: There are more than two connections from either a single ISP or more than one ISP. When there is more than one ISP, it is due to fault tolerance so that if one ISP fails, the other ISP continues to function. It is also to use the best route provided by any of the ISPs.
- Dual Multi-Homed: There are two connections from several ISPs. This is implemented when you need to have a high level of redundancy.

# Default Route

- Is a static route that is defined in the routing table
- Is also known as the default gateway
- Is used when no route to the destination is found and the destination address is unknown
- Is designated as:
  - IPv4: 0.0.0.0/0
  - IPv6: ::/0

```
Router(config)#ip route 0.0.0.0 0
```

```
Router#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2
      i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
      ia - IS-IS inter area, * - candidate default, U - per-user static route
      o - ODR, P - periodic downloaded static route

Gateway of last resort is 192.168.1.2 to network 0.0.0.0

      10.0.0.0/24 is subnetted, 1 subnets
S        10.10.10.0 [1/0] via 192.168.1.2
C        192.168.1.0/24 is directly connected, FastEthernet0/0
S*       0.0.0.0/0 [1/0] via 192.168.1.2
```

In dynamic routing, you had learned the term default route, which is the static route defined in the routing table. It is also known as the gateway. If there is no knowledge of any known route to the destination, the default route sends out the information.

For example, there is a default gateway in a network, which is the default route provided by the ISP. It is the only destination to which the packets are sent. In simplest terms, to understand a default route, another router's IP address is most likely installed at the ISP's location.

The default route differs in IPv4 and IPv6 due to their addressing format differences.

- IPv4: 0.0.0.0/0
- IPv6: ::/0.

The default route is usually configured on the edge router, located at the entry or exit point of a network.



# Administrative Distance

- Can be assigned manually or dynamically
- Is used to select the routing protocol if two of them are used to get to the same destination
- Uses a range from 0 to 255 – lower the number, better the route is
  - 0 = Best
  - 255 = Worst (discard)
- Does not add the route that has the source with administrative distance of 255

Route Source	Default Distance Values
Connected interface	0
Static route	1
Enhanced Interior Gateway Routing Protocol (EIGRP) summary route	5
External Border Gateway Protocol (BGP)	20
Internal EIGRP	90
IGRP	100
OSPF	110
Intermediate System-to-Intermediate System (IS-IS)	115
Routing Information Protocol (RIP)	120
Exterior Gateway Protocol (EGP)	140
On Demand Routing (ODR)	160
External EIGRP	170
Internal BGP	200
Unknown*	255

Assume that you have a router that is configured with two routing protocols. When a packet needs to be delivered, the router has to choose one routing protocol. The administrative distance that the router uses to determine the best routing protocol to use for sending out information to the destination.

In simplest terms, an administrative distance is the reliability of a routing protocol. You must note that the administrative distance is never shared by a routing protocol when it is sharing its routing table or routing information. The administrative distance information is retained locally by a router to decide the best routing protocol.

Each routing protocol has an administrative distance value. The smaller the administrative value, the more reliable the routing protocol is. A router will always choose the routing protocol with the smallest administrative value over the one with a higher administrative value. For example, if a router has to choose between OSPF or IGRP, it would go with the IGRP because its administrative distance is smaller than OSPF. The administrative distance for IGRP is 100, and for OSPF, it is 110.

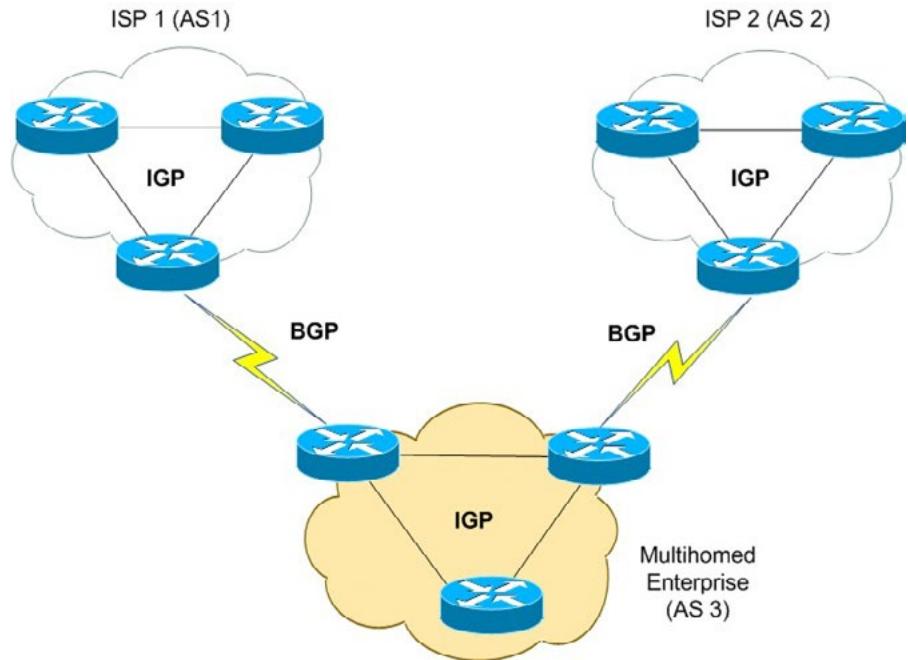
The administrative distance value starts from 0, which is assigned to the connected interface. It goes up to 255, which is unknown. The route source with an administrative distance of 255 is never trusted and added to the routing table.

Even though each routing protocol has an administrative distance, you can still modify this value.



# Exterior vs. Interior

- Interior Routing
- Takes place within a single network known as autonomous system
- Can use one or more protocols for routing
- Examples:
  - RIP
  - OSPF
  - EIGRP
- Exterior Routing
- Takes place between different autonomous systems
- Can use only one routing protocol for routing
- Examples:
  - BGP



Routing is of two types: internal and external. When you refer to the internal routing, it is restricted within a single autonomous domain. There are routing protocols that are meant to be used only for internal routing. Some of the key internal routing protocols are:

- Routing Information Protocol (RIP)
- Open Shortest Path First (OSPF)
- Enhanced Interior Gateway Routing Protocol (EIGRP)

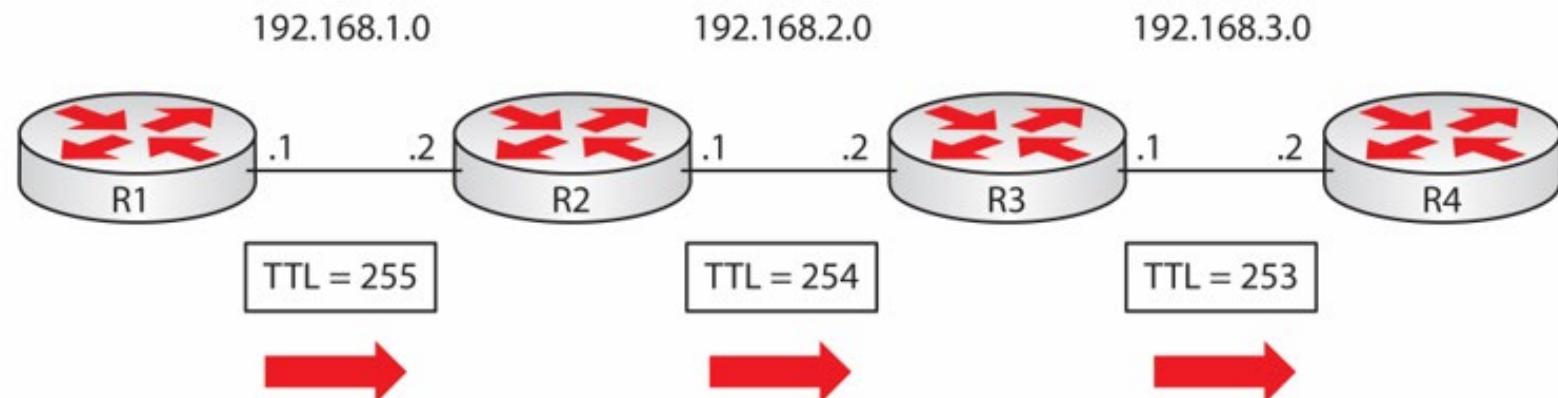
It is possible to use more than one routing protocol in internal routing.

External routing takes place between two or more autonomous domains. You can only use one routing protocol in external routing. An example of an external routing protocol is:

- Border Gateway Protocol (BGP)

# Time to Live

- Is an 8-bit fields in the IP header
- Is assigned by the source system before sending the packet to the destination
- Requires a value greater than 0 to be sent forward to the next router
- Has the following ranges:
  - 0 is restricted to the same host
  - 1 is restricted to the same subnet
  - 32 is restricted to the same site
  - 64 is restricted to the same region
  - 128 is restricted to the same continent
  - 255 is unrestricted



# Time to Live

Time to live, more commonly known as TTL, is when a packet lives or exists on the network before it is discarded. The TTL value is assigned by the system that initiates the communication with the destination host. You can call it a packet's lifetime on a network before it is discarded.

Each packet that is sent on the network has a TTL embedded, which is the predefined timespan. There is a reason for having the predefined timespan. Consider a scenario in which the timespan value is not defined. The packet will keep moving indefinitely and will never be discarded.

Let's see what this 0 means. Each hop on which the packet travels, it decrements the TTL value by 1. If a packet is initiated with the TTL value of 1, it will be discarded on the first hop itself as the value of 1 is decremented by 1, which eventually leaves 0.

There are default TTL values that are assigned. Any packet with the TTL of 0 is immediately discarded as it is restricted only to the host that initiated the communication.

TTL Value	Restricted to
	0
Same host	
	1
Same subnet	
	32
Same site	
	64
Same region	
	128
Same continent	
	255
Unrestricted	

When you execute the command, you can see the TTL value in the output. For example:

Pinging google.com [142.250.193.206] with 32 bytes of data:

```
Reply from 142.250.193.206: bytes=32 time=6ms TTL=117
Reply from 142.250.193.206: bytes=32 time=8ms TTL=117
Reply from 142.250.193.206: bytes=32 time=9ms TTL=117
Reply from 142.250.193.206: bytes=32 time=9ms TTL=117
```



*TOPIC 2*

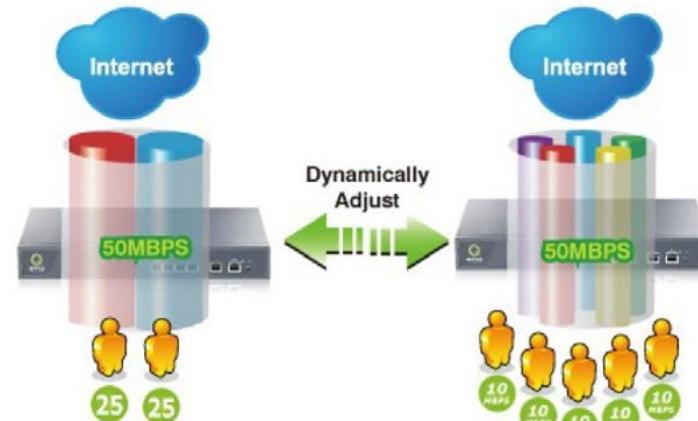
---

# BANDWIDTH MANAGEMENT

---

# Bandwidth Management

- Is a process of controlling the use of bandwidth on a network or Internet link
- Is performed to avoid bandwidth overutilization by a particular application or protocol
- Is performed to avoid network congestion
- Helps to restrict the application to use a specific amount of bandwidth



[Bandwidth Management \(infotek.id\)](http://infotek.id)

A network can run a variety of applications. Each application needs some amount of bandwidth to run its services. In most cases, the bandwidth is over-consumed because it is not managed properly. Each application may run to consume as much as possible, resulting in a bandwidth crunch. The solution to bandwidth overutilization or crunch is bandwidth management.

Bandwidth management is a method of controlling bandwidth on a network or over the Internet link. You can allocate a specific amount of bandwidth to applications or, in some cases, to the protocols. For example, you can limit the maximum bandwidth consumed by an FTP application to be 5 Mbps. In this case, no matter how much data needs to be sent to an FTP server, it is always limited to maximize bandwidth utilization, which is 5 Mbps.

When bandwidth is managed by capping, it helps to avoid network congestion and overutilization. Each application gets only the allocated share.

# Traffic Shaping

- Is applied only for the outbound traffic
- Queues up the excess traffic and schedules its delivery
  - Queues only within the defined limit
  - Buffers the excess packet that can cause delay
- Prioritizes the traffic for time-sensitive applications
- Helps to enhance traffic as it can categorize and queue up traffic

*Traffic Shaping (Packet Shaping)*



[T Archives - Avi Networks](#)

Traffic shaping is the method of controlling the speed of the outflow of traffic. When you are sending outbound traffic, sometimes you need to limit its speed. You apply traffic shaping only on the outbound traffic by putting a specific bit rate on it to not outflow with a maximum speed of the NIC, such as 1 Gbps.

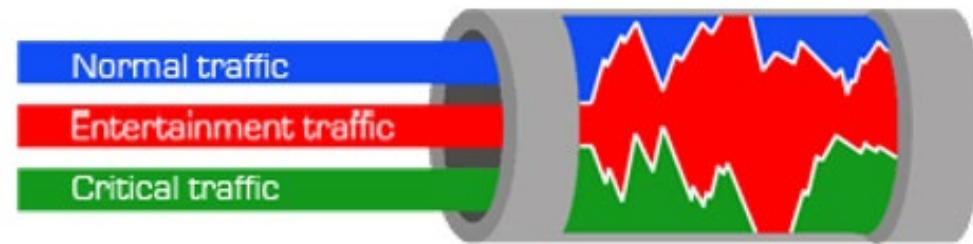
When you apply traffic shaping, the maximum speed limit is assigned to the outgoing traffic. You have 1 Gbps NIC, but you limit the traffic speed to only 500 Mbps. When the traffic starts to outflow, it gets restricted to 500 Mbps, but what about the rest of the traffic that was to go at 1 Gbps? It gets queued up till the remainder of the time, after which the queued-up data is sent. However, when the excess data, the remaining 500 Mbps, get queued up, it must wait to be delivered. This can cause a delay in sending the data.

With the traffic shaping, you can prioritize the traffic for latency-sensitive applications, which are impacted due to high latency.

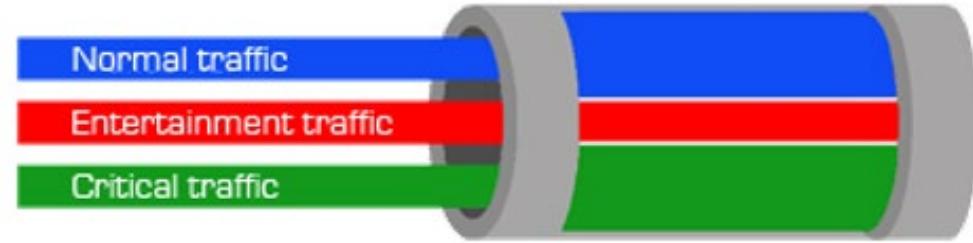
# Quality of Service (QoS)

- Is a method of prioritizing different types of network traffic
- Identify and mark the traffic
- Segregate it
- Enables the administrator to:
- Predict the use of bandwidth
- Monitor and control the use of bandwidth
- Divert the bandwidth to time and latency-sensitive applications
- Ensures efficient usage of the network bandwidth
- Prioritize the applications like Voice over IP
- Assign low priority to the latency-insensitive applications like File Transfer Protocol (FTP)

Bandwidth Use without QoS control



Bandwidth Use with QoS control



# Quality of Service (QoS)

A network can have a variety of traffic. If there is no proper traffic management, then each type consumes as much traffic as it can. Therefore, as one of the bandwidth management techniques, you can use Quality of Service or more commonly known as QoS. If a certain type of traffic requires more priority over the other, you can use QoS to handle such requirements.

A network administrator needs to identify the types of traffic in the network and segregate them so that the appropriate traffic, such as voice, can be given high priority. Voice traffic needs more bandwidth. Therefore, you should use the voice infrastructure in a separate virtual LAN or VLAN and prioritize this traffic. The rest of the normal traffic, like data, can be given low priority. This will ensure optimal bandwidth available for the voice traffic, and it does not suffer from bandwidth crunch.

QoS provides several benefits, such as enabling the administrator to predict bandwidth use and enabling better control and monitoring. QoS works at Layer 2 and 3 of the OSI model. The routers and switches need to have QoS enabled to be able to handle such traffic.

There are certain applications, such as voice and video, that are latency-sensitive. If there is high latency in-network, you will not get the voice or the video. For example, if you are trying to watch a video on YouTube, it fails to load or gets stuck in between. This is the case of high latency. You would surely want the video to play without any issue. QoS can help you achieve this goal. This is the case of a latency-sensitive application that requires bandwidth for speedy delivery. VoIP is another example of a latency-sensitive application.

Then, other applications do not require care for the latency. These applications are known as latency insensitive. They will continue at a slow speed. For example, file download or File Transfer Protocol (FTP) are two examples. However, they do impact latency-sensitive applications.

It is also evident that a network will most likely always have latency-sensitive and latency insensitive applications. You need to prioritize the latency-sensitive applications over the latency-insensitive ones.

# Summary

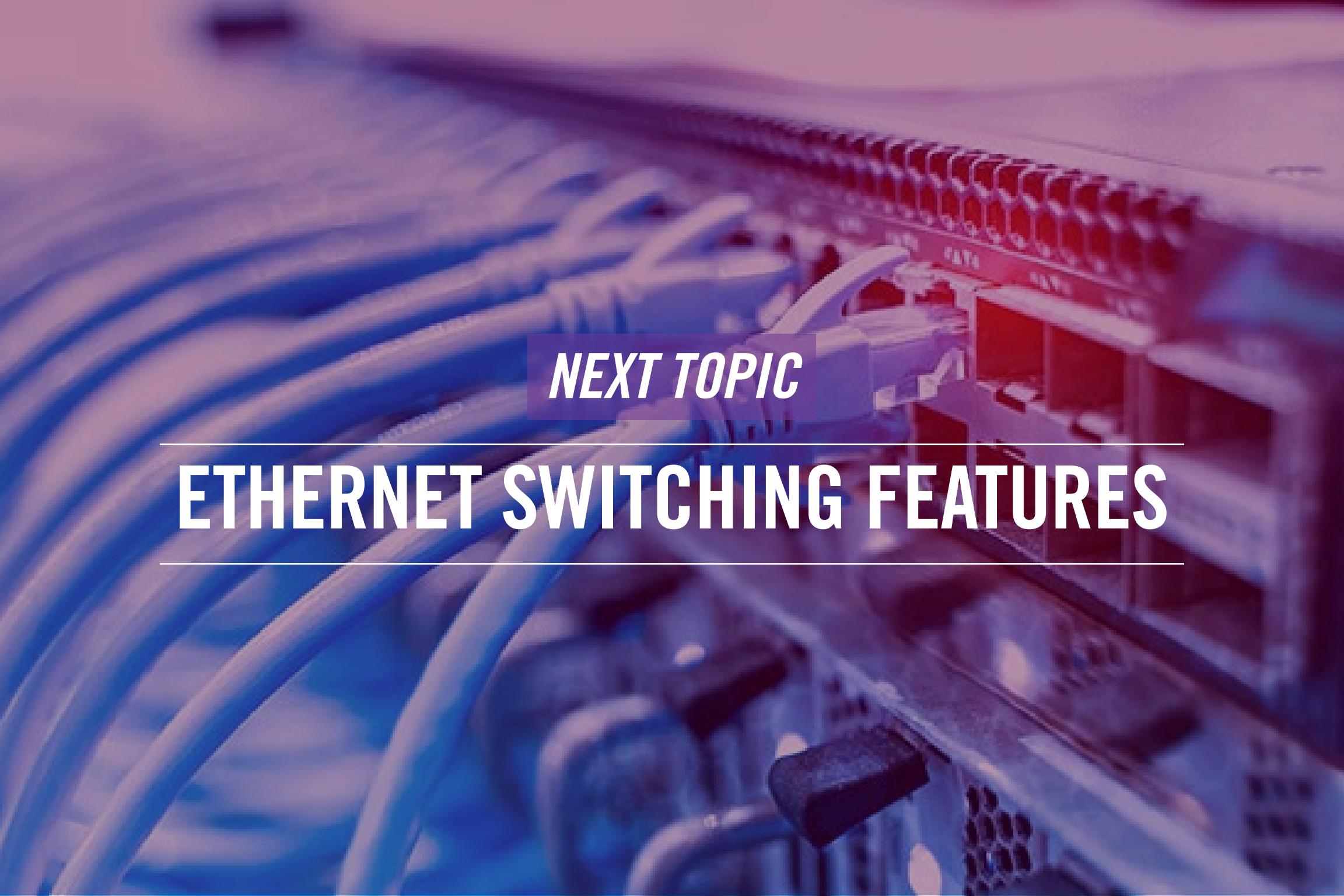
- Routing
- Bandwidth Management



That's the end of the lesson.

Here we covered:

- Routing
- Bandwidth Management



**NEXT TOPIC**

---

# ETHERNET SWITCHING FEATURES

---

Lesson

3

---

# Ethernet Switching Features

- 1 — Welcome to the lesson 3 of Module 2. In this lesson, you will learn about the:
  - 2 — Ethernet Switching Features
- 



Network Fundamentals

# AGENDA

- Ethernet Switching Features



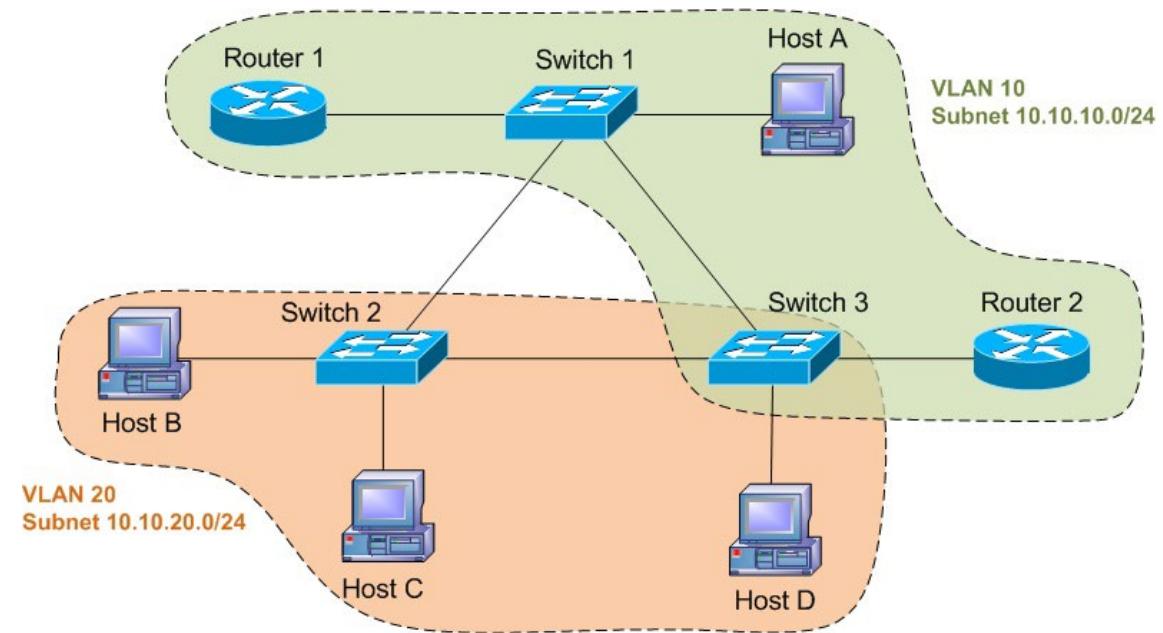
Hi, welcome to COMPTIA Network+ Course  
In this lesson we will talk about:

- Ethernet Switching Features



# Data Virtual Local Area Network (VLAN)

- Is a network that groups a set of systems with similar purpose
- Limits the broadcast traffic within itself
- Reduces the excess network traffic and collisions
- Can be configured across one or more switches as long as they have a single broadcast domain
- Can be different types, such as Management VLAN, Data VLAN, and Voice VLAN



# Data Virtual Local Area Network (VLAN)

Fundamentally, a virtual local area network (VLAN) is a network or part of a network that groups a set of systems with a similar purpose. A VLAN, in simplest terms, is a group of ports on a switch that binds the systems together into a smaller network. When the systems are part of this network, they can interact without a gateway or an intermediate entity.

A VLAN also restricts the broadcast traffic within itself. Each VLAN that exists is a broadcast domain, which eventually reduces the excess network traffic and collisions. Think of a large network without VLAN. It would be unimaginable even to think the amount of broadcast traffic is generated. Each device is getting broadcast traffic. It will eventually be overwhelming for the device to keep getting the broadcast traffic.

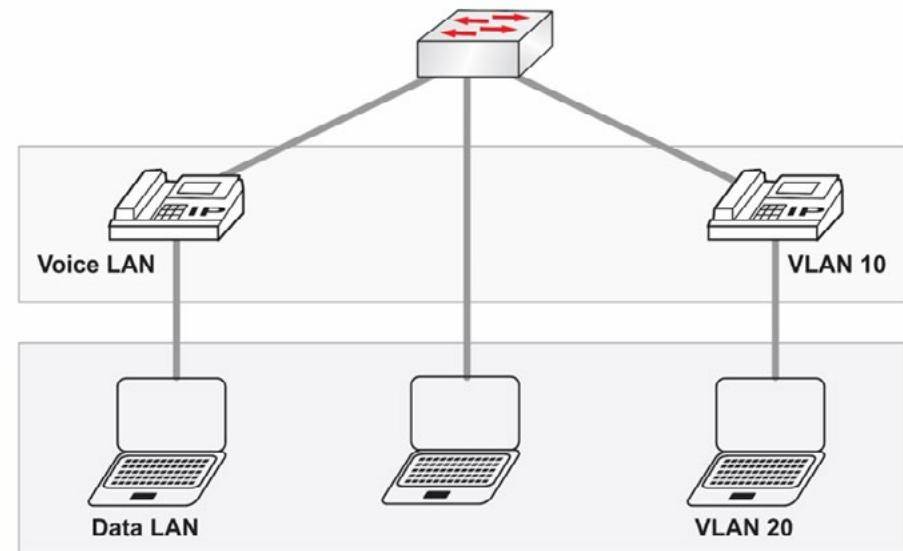
Most often, people confuse the terms subnets with the VLANs. A subnet is a logical division of a network based on the IP addresses. When you subnet a large network, you have several smaller networks in which each network is assigned a range of IP addresses. The communication between these networks is through the Layer 3 switches or the routers.

On the other hand, a VLAN is configured on a Layer 2 switch, not routing capabilities. You take several ports and club them as a VLAN on the switch. Each VLAN uses a router to send out the traffic. A router does not accept the broadcast traffic, and therefore, it is restricted within the VLAN. It is not necessary to have a VLAN in a single physical location on a floor. You can use several switches to create a single VLAN, which may be spanned through several floors.

There can be several types of VLANs that you can create. You can create a data VLAN, which is mainly used for users who generate data. In most cases, you will create a data VLAN. Another type of VLAN that you can create is a voice VLAN, which will contain the Voice over IP (VoIP) infrastructure. Another type of VLAN is the management VLAN, which contains devices and applications used to manage a network and its devices.

# Voice VLAN

- Is a separate VLAN that contains the VoIP infrastructure
- Helps to preserve the traffic within the same broadcast domain
- Is designed for voice streams that are given high priority over other VLANs
- Can identify the traffic in two different ways by identifying:
  - Source MAC addresses of the received packets
  - VLAN tags of the received packets



A voice VLAN contains the VoIP infrastructure that is used for generating voice traffic. In an organization, several users often use VoIP phones or voice-related applications, such as softphones. When a user makes a call, the voice is converted into data streams and sent to the destination network. This needs to be segregated into a separate VLAN so that these data streams do not create congestion on the data network. It also helps to contain the broadcast traffic within the same VLAN where it originated.

One of the critical intents of creating a voice VLAN is prioritizing voice traffic over other types of traffic. VoIP runs over the UDP protocol, and if there are delays or network congestion, it degrades the voice quality. Therefore, it is better to segregate the voice traffic from the others and assign it a high priority.

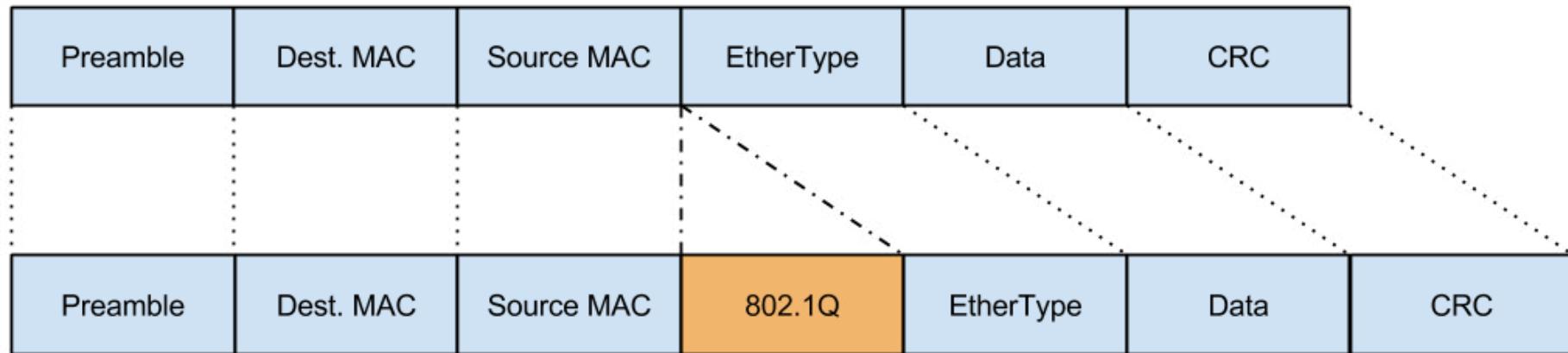
Let's look at the graphic on the slide. When a voice packet is sent, the voice VLAN information is added, and then the packet is sent. The tagged voice packet is assigned high priority over the other traffic. You are identifying the voice packets from the rest of the traffic. The identification can be made in two different ways:

MAC address-based mode: a network switch determines whether a data packet is a voice packet or not. It checks for its source MAC address and then matches it with the Organizationally Unique Identifier to determine if the matched MAC is from the voice VLAN. If the MAC address matches, the data packet is then tagged, and priority is raised.

VLAN-based mode: A network switch verifies the VLAN ID of the received packet. The switch tags the packets with the voice VLAN information and sends the packet back to the device, which is a VoIP phone. The VoIP phone again sends the packets back to the switch, verifying whether it contains the voice VLAN information. If the packet contains the voice VLAN information, then it is assigned high priority.

# Port Configuration - Port tagging/802.1Q

- Allows a switch port to receive traffic from more than one VLAN
- Inserts a tag in the packet header between the Source MAC and EtherType fields
  - 802.1Q that contains the destination VLAN address
- Is able to determine the destination with the destination VLAN address



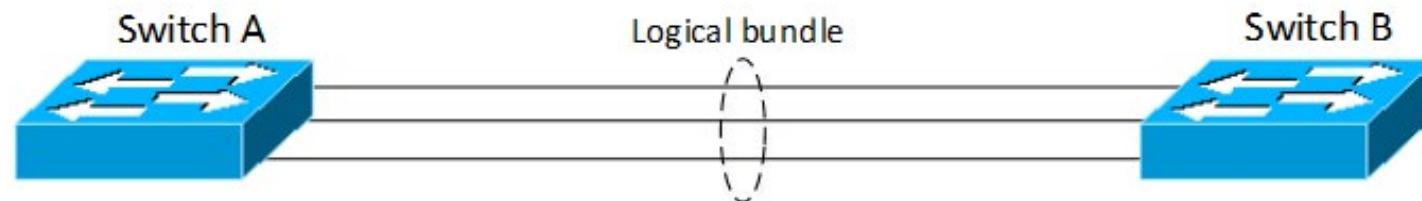
[Why and how are Ethernet Vlans tagged? - Network Engineering Stack Exchange](#)

Each port on a switch is typically assigned to a single VLAN, which means it is part of a single broadcast domain. However, a single switch port can be configured to send and receive traffic from more than one VLANs at once with port tagging. For example, let's say that you have a file server that needs to cater to several VLANs at once. It needs to be accessible to the Accounting, Production, and Senior Management VLANs. In such a case, the packets going out of this port need to determine their VLANs. They should be able to reach the correct VLAN.

To do this, a tag is inserted in the packet header between the Source MAC and EtherType fields. This field is called the 802.1Q field that contains the destination VLAN information. When a frame is out on its way, the 802.1Q field is verified to determine the destination VLAN information.

# Port Configuration - Port Aggregation

- Is a method of combining two or more ports
- Allows the combined ports to act as a single logical port
- Can be performed in one of the following ways:
  - Auto
  - Desirable
  - On
- Is called link aggregation group when you combine multiple ports (Etherchannels/PAgP/LACP)



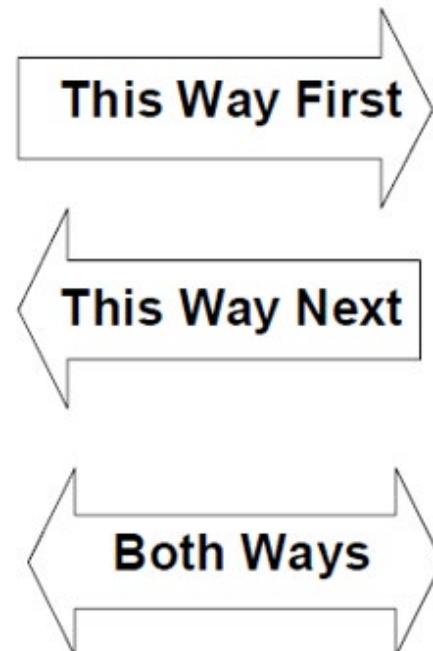
Port aggregation is a method of combining two or more ports on a switch. Port aggregation is performed using the Port Aggregation Protocol (PAgP), a Cisco proprietary protocol. With the method of port aggregation, when multiple ports are combined, several benefits are gained. One of the key benefits is the increase of throughput, which is also increased by adding the throughput of the individual ports. The second benefit is the implementation of redundancy. In case one of the ports fails, the remaining ports can continue to work. When the data is received or sent, it is done via a single logical port, which is the outcome of the port aggregation method.

There are three modes in port aggregation:

- Auto Mode: Works by responding to the packets sent by the other end.
- Desirable Mode: Initiates the negotiation with the other end.
- On Mode: Is used when both the end devices have On mode enabled.

# Port Configuration - Duplex

- Can be of two types:
  - Half Duplex
  - Full Duplex
- Half Duplex
  - Enables only unidirectional traffic flow
  - Has possibility of collision
- Full Duplex
  - Allows the traffic to flow bi-directional – to and fro at the same time
  - Reduces the transmission time because data is flowing back and forth simultaneously
  - Requires the sender and receiver to enable full duplex mode



**HALF DUPLEX -  
ONE WAY AT A TIME**

**FULL DUPLEX -  
BOTH DIRECTIONS  
AT THE SAME TIME**

# Port Configuration - Duplex

A switch works with a specific mode known as a duplex, which decides how the traffic is sent to the nodes on the network or how the communication needs to be performed. For example, duplexing decides whether the communication needs to be through a single channel or bi-directional. A switch and the communicating device should be configured to work on the same duplex setting. For example, a system on the network and switch need to talk at the same speed rather than one talking very fast and another very slow and not understanding what the other party is saying.

The duplex settings are of two types, half-duplex and full-duplex.

## Half-duplex

Half-duplex works with unidirectional traffic. This means that it can either receive or send traffic at any given time, but it cannot send and receive at the same time. A system with a half-duplex setting has to wait to send data when receiving it from another system on the network. This causes delay and possible collision. If a switch port is configured in full-duplex, but the system is configured with half-duplex, the switch will also need to work with the half-duplex. Half-duplex is usually performed with CSMA/CD to detect collision.

## Full-duplex

With full-duplex, the communication is bi-directional. A switch or a system can send and receive data at the same time. The receiving traffic and sending traffic go through different channels, and therefore, there are no chances of collision. When you enable the full duplexing mode, the CSMA/CD mode is automatically disabled.

With a full duplex, because the sending and receiving of data packets are performed simultaneously, the transmission time is reduced. The device does not have to wait to finish sending and then start receiving or vice versa. Both the tasks can be performed at the same time.

Both the sender and receiver need to have full-duplex mode enabled.



# Port Configuration - Speed

- Varies to different speeds:
  - 10 Mbps
  - 100 Mbps
  - 1000 Mbps
- Half-duplex
  - 10 Mbps
  - 100 Mbps
- Full-duplex
  - 100 Mbps
  - 1000 Mbps
- Auto – Uses 10 Mbps and half-duplex if speed is not known

```
Router(config-if)#speed ?
      10    Force 10Mbps operation
      100   Force 100Mbps operation
      auto  Enable AUTO speed configuration
```

Along with the duplex setting, you also need to pay attention to the speed settings on a switch and the receiving devices, such as systems on the network. There is usually an auto-negotiation between the switch and the device to work at the same speed, such as 100 Mbps or 1000 Mbps. Both of them need to agree on the same speed.

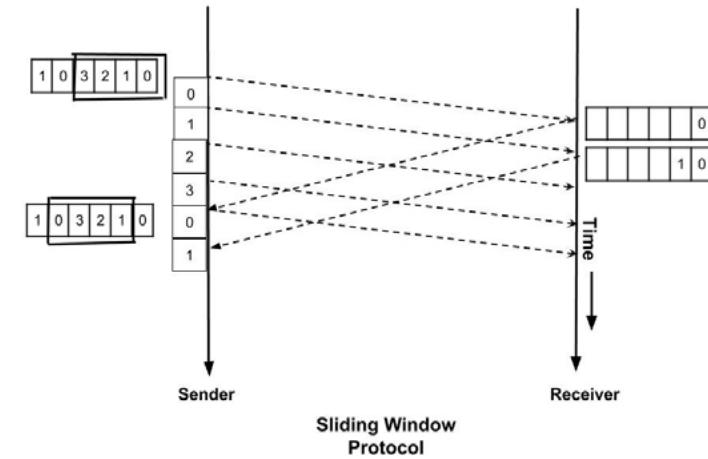
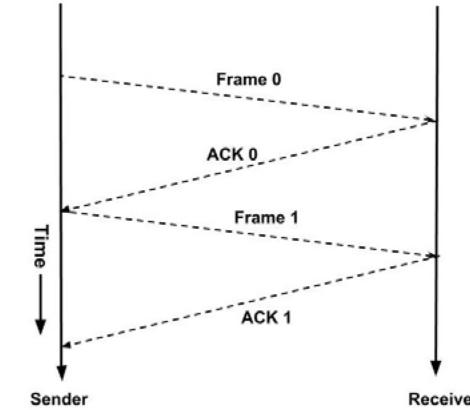
Let's take an example of a switch and a device—the switch support 1000 Mbps or 1 Gbps. However, the device can only work at 100 Mbps. In this case, not only the duplex settings are matched but also the speed. The switch will need to work at the 100 Mbps speed because the device, for obvious reasons, cannot work on the 1000 Mbps.

If both the switch and the device are set to auto-negotiation and speed cannot be determined, the communication occurs at 10 Mbps and half-duplex.



# Port Configuration – Flow Control

- Is a method used by a sender interface to match the speed of the recipient interface
- Requires the sender interface to slow down if recipient cannot receive transmission on the same speed
- Can use one of the following two protocols:
  - Stop and Wait Protocol
  - Sliding Window Protocol



[What is Flow-Control in networking? \(afteracademy.com\)](http://afteracademy.com)

# Port Configuration – Flow Control

In the previous slide, you learned about the speed, which must be matched between the switch and the device to communicate. The flow control method prevents the sender from sending data at a higher speed than the receiver can accept. It can be communication taking place between a switch and a device or two devices on the network.

In this method, a receiver has a fixed buffer size to accept a certain amount of data. The sender has to wait for the receiver to send an acknowledgment to send more data. When the sender sends the data, the flow control method prevents the sender from keeping sending data.

Imagine a scenario in which the sender keeps sending more data than the receiver can receive. What is likely to happen to this data? It is going to get lost, and the sender will not be able to receive it. Flow control makes the sender wait until the receiver sends an acknowledgment that it can receive more data.

Flow control can use one of the two protocols:

- Stop and Wait Protocol:
- Sliding Window Protocol

## Stop and Wait Protocol

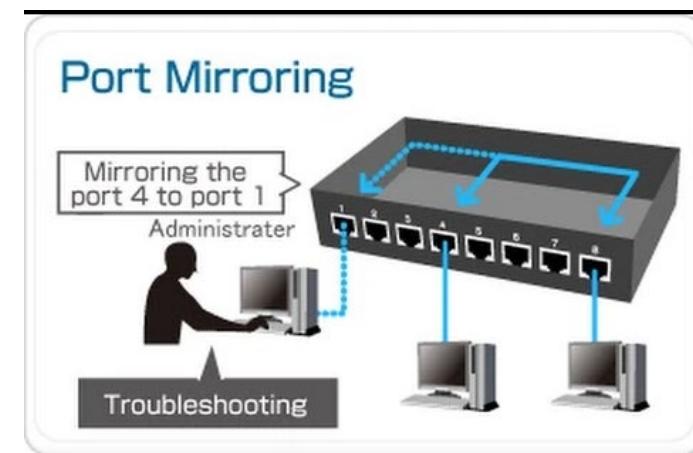
A sender sends a packet to the receiver, which has to send an acknowledgment to the receiver. Until the sender receives the acknowledgment, it cannot send more packets to the receiver. However, the sender does not wait forever to send the next packet. There is a wait time for the sender to wait for the acknowledgment. When the wait time is over and acknowledgment is not received, it sends the packet again. It is important to note that the sender can send only one packet with the Stop and Wait for protocol, which also increases the transmission time as there is a wait for the acknowledgment from the receiver.

## Sliding Window Protocol

A switch or any sender sends several frames in one go. When the receiver receives the first frame, it sends the acknowledgment back to the sender. Then the second frame is immediately sent. The critical point to consider is that several frames are sent in one single window. As acknowledgments are received, the next frame is being sent to the recipient.

# Port Configuration – Port Mirroring

- Is a method of sending received traffic on a switch to the connected device on a port
- Enables the replication of the complete switch traffic through the port on which the device is mapped
- Is useful to troubleshooting network issues
- Types of port mirroring:
- Switched Port Analyzer (SPAN)
- Remote Switched Port Analyzer (RSPAN)
- Encapsulated Remote Switch Port Analyzer (ERSPAN)



Port mirroring monitors the network by attaching a device or system that has the network monitoring application installed. A port with a connected device or system on a switch copies all the traffic received on the switch. This port intends to copy all the incoming traffic on the switch.

An important point to note is that there is no alteration to the received traffic. The port simply copies the complete received traffic and sends it to the connected device, which need not be physically connected to the port. It can be anywhere on the network but needs to be mapped to the port configured for port mirroring.

You can capture the traffic for monitoring purposes. The captured traffic can also be saved and later analyzed for any kind of network anomalies. Port mirroring can be enabled in:

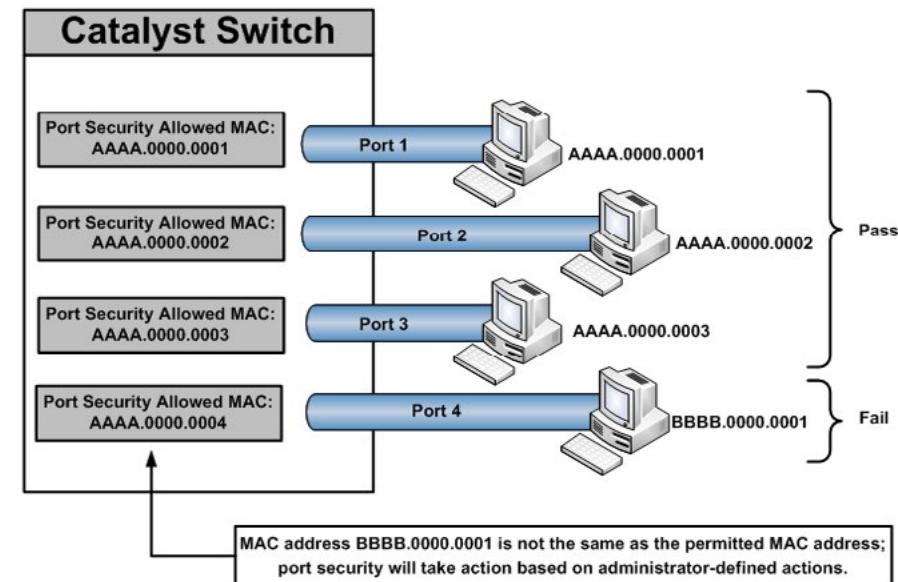
- A Local Area Network (LAN)
- A Virtual Local Area Network (VLAN)
- A Wireless LAN (WLAN)

There are three different types of port mirroring:

- Switch Port Analyzer (SPAN) – the monitoring device is connected to the port.
- Remote Switch Port Analyzer (RSPAN) – the monitoring device is not physically connected to the port. It can be located anywhere on the network.
- Encapsulated Remote Switch Port Analyzer (ERSPAN) – It is an advanced version of RSPAN. The captured traffic is sent to the device using Generic Route Encapsulation (GRE).

# Port Configuration – Port Security

- Works at Layer 2 of the OSI model
- Binds specific addresses to the ports to allow only authorized MAC addresses to use them
- Prevents the misuse of unused ports by disabling them
- Allows only the MAC addresses that are stored in the MAC Address Table
- Shuts down the port if there is a violation



In most cases, a switch will have several ports that are available and free for use. These ports can be misused if they are not appropriately secured. For example, anyone can plug a malicious laptop into the port and release malware or capture network traffic. To secure the free ports, you need to configure port security, mapping one or more MAC addresses with the specific ports.

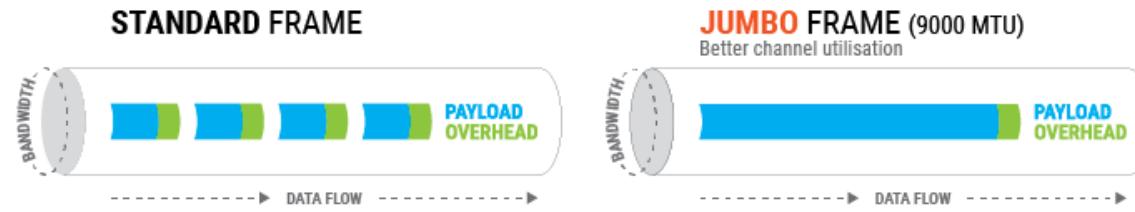
Port security works at the Data Link Layer, which is Layer 2 of the OSI mode. Port security requires the use of managed switches, which the administrator configures for better control and usage of the switch. With the port security, you can limit which MAC addresses can use a specific port. You can also increase the port security by disabling them when they are not in use.

It is also essential to understand that the administrator can configure different actions for port security. For example, if a violation of any kind involves a port, it can be shut down automatically.

In the given graphic, only two MAC addresses are allowed to connect to a port. Therefore, the third MAC address, which belongs to Host B, is denied access.

# Port Configuration – Jumbo Frames

- Has a payload larger than the standard size, which is 1500 bytes
- Can be up to 9000 bytes
- Are used in networks with 1 Gbps speed
- Improves network performance as there are less frames to transmit
- Must be configured on the device to send and receive



[Jumbo Internet Exchange IPTP Networks](#)

As and when a packet moves on to the network, there are chances that its default payload size, which is 1500 bytes, is modified to accommodate more information. For example, an additional piece of information may be added to the header, or any filtering information may be added. It becomes difficult to accommodate additional information into the default frame size. Additional data means more data needs to process.

This is where jumbo frames come into the picture. They can have a size up to 9000 bytes, which means they can accommodate much more information than the standard size. This helps reduce the number of packets, but larger packets are being sent at the same time.

Jumbo frames are used in high-speed networks that have at least 1 Gbps speed. When a switch or a router receives packets, it can process only one packet at a time. Smaller packets will be much large in number, so the CPUs on the switches or routers have to process them one by one. This adds CPU overhead. On the other hand, when there are jumbo frames, they are much more prominent in size, accommodating more information. Because the information is accommodated in only a few jumbo frames, there is less effort that the switches and routers have to process them.

The sender and the receiver devices must have jumbo frames enabled. If the sender has and the receiver does not, they will drop these packets or fragment them. This may put additional overhead on the CPUs of the switches and routers.

# Port Configuration – MDI-X

- Stands for auto-medium-dependent interface crossover
- Performs an automatic detection at the other end to select MDI or MDI-X
- Detects if the connection requires a crossover and automatically selects to use MDI or MDI-X
- Use cases for MDI and MDI-X
  - MDI: desktops, routers, and servers
  - MDI-X: hubs, switches, and bridges



[Medium-dependent interface - Wikiwand](#)

MDI-X stands for auto-medium-dependent interface crossover, which is an extension of Medium Dependent Interface (MDI). MDI-X performs an automatic detection to check if the network connection requires a crossover. Based on the outcome, it then selects either MDI or MDI-X.

Either MDI or MDI-X cable decides the type of cable you use. You would use the MDI with the end device, such as desktops, routers, and servers. On the other hand, MDI-X is used with the networking devices that enable the transmission of traffic. Such devices are hubs, switches, and bridges.

Switches and routers have several MDI-X ports and one MDI port. The primary purpose of MDI-X is to detect whether the end device initiating the connection requires an MDI or MDI-X interface. Depending on the type of interface, MDI or MDI-X, you can select the correct type of cable to use. For example, you need to use a straight cable to connect an MDI port to an MDIX port, such as an end device to a switch. However, when you need to connect MDI-to-MDI, such as two systems, or MDIX-to-MDIX connections, such as two switches, you need to use the crossover cable.

# Media Access Control (MAC) Address Tables

- Stores the MAC addresses
- Is used by a switch to send out a frame to the correct destination
- Is updated by a switch in case a MAC address is not available
  - Switch floods all ports except from the port it received the frame
  - Switch updates the MAC address table when it receives the response from the destination

```
Switch#show mac address-table
```

Mac Address Table

Vlan	Mac Address	Type	Ports
---	-----	-----	-----
1	0001.42dd.eca1	DYNAMIC	Fa0/1
1	0001.c7d2.4eb1	DYNAMIC	Fa0/2
1	00e0.f9de.e036	DYNAMIC	Fa0/3

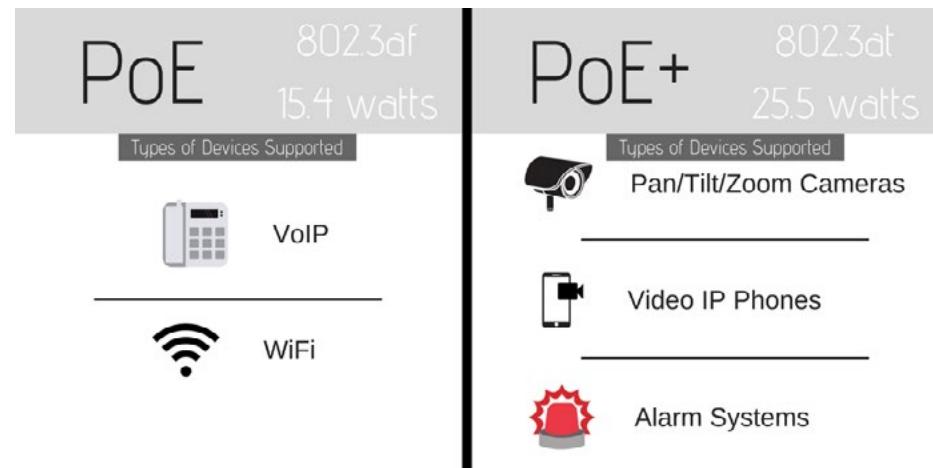
From the previous lessons, MAC address stands for Media Access Control, a globally unique 12-digit number assigned to a network interface card (NIC). MAC addresses are used by the switches to identify the target to which the packets need to be sent. A switch keeps the MAC addresses in the MAC Address Table and continues to update it when it learns about the new MAC addresses.

The switch maps the ports with the MAC addresses. For example, if a switch receives a frame from a specific port, it updates its MAC address table with the sender's MAC address. It then checks for the MAC address of the recipient device. If it finds, then it sends the frame to the mapped port of this MAC address. If it does not find the MAC address in the MAC address table, it sends the frame to all ports except the port that had received the traffic. Whenever the correct port responds, it then maps the port with the MAC address of the recipient device.



# Power over Ethernet (PoE)/POE plus (PoE+)

- POE
- Uses the twisted-pair Ethernet cable to deliver power to the networking devices, such as:
- Wireless Access Point
- VoIP phone
- Uses the Ethernet cable to transfer power and data at the same time
- Can supply up to 15.4 watts of electricity to the devices
- POE+
- Provides maximum power of 30W
- Provides 25.5W to the powered device
- Can be used with cameras, VoIP phones, and alarm systems



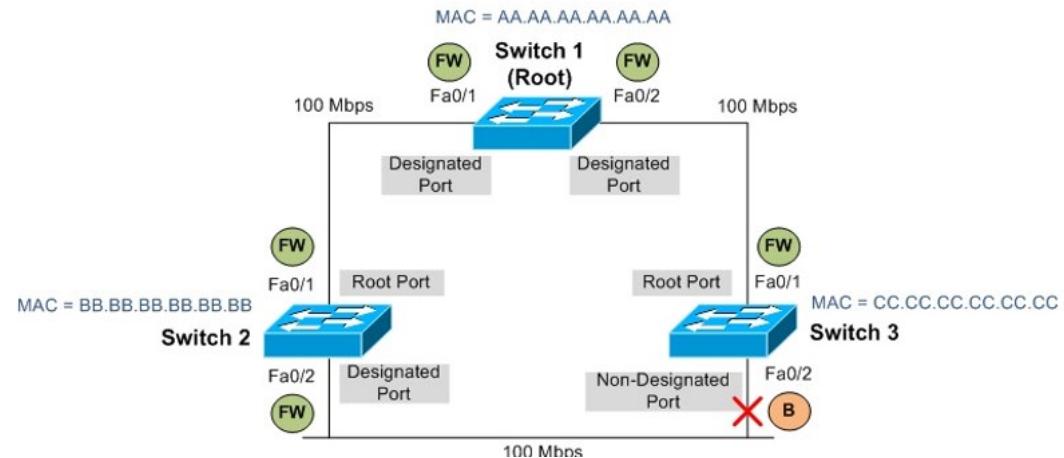
Most of the network equipment requires power or electricity to function. Such devices can be powered with the Ethernet cable if they have the Power over Ethernet (POE) or POE+ capabilities. However, there may be situations when a power socket is not available within the reach of the installed wireless access point (WAP) because it is stationed on a height.

With POE, you can use a twisted-pair Ethernet cable to deliver the power to the network device, such as a VoIP phone or WAP. In this case, no separate power source is required. The Ethernet cable is used for both the data and the power. PoE can supply 15.4 watts of electricity to the device. It can be used with WAPs and VoIP phones.

PoE+ is the advanced version that can supply up to 30 watts to the network devices. Out of the 30 watts, it can supply up to 25.5 watts to the devices. It can be used with cameras, VoIP phones, and alarm systems.

# Spanning Tree Protocol (STP)

- Is used to prevent switching loops between devices, which can occur because of multiple paths available to a destination
- Uses the Spanning Tree Algorithm (STA) to prevent loops in a network
- Ensures only one active path is available for transmission even if multiple paths are available
- Sends the data only on the approved path



Assume that you are driving to a destination that has multiple routes available. You would, for obvious reasons, be confused about which routes to take. You might end up taking a longer route or a route that has much congestion.

Similar things happen in the networks also. There may be multiple network paths available on the network, which may cause loops. Multiple network paths are used chiefly for redundancy purposes. The STP protocol enables only one active network path to prevent loops. The STP protocol uses the Spanning Tree Algorithm (STA) responsible for creating the spanning tree. If a switch fails, then STA creates a new spanning tree. STA creates the topology database that STP uses to look for paths or links.

STP uses the bridge protocol data units (BPDUs) to keep track of the ports' status on a switch. BPDUs are exchanged between the switches to keep track of the port status. If there is an issue with the port or a loop in the network, the port is shut down. Various other actions can be performed, such as blocking it or disabling it.

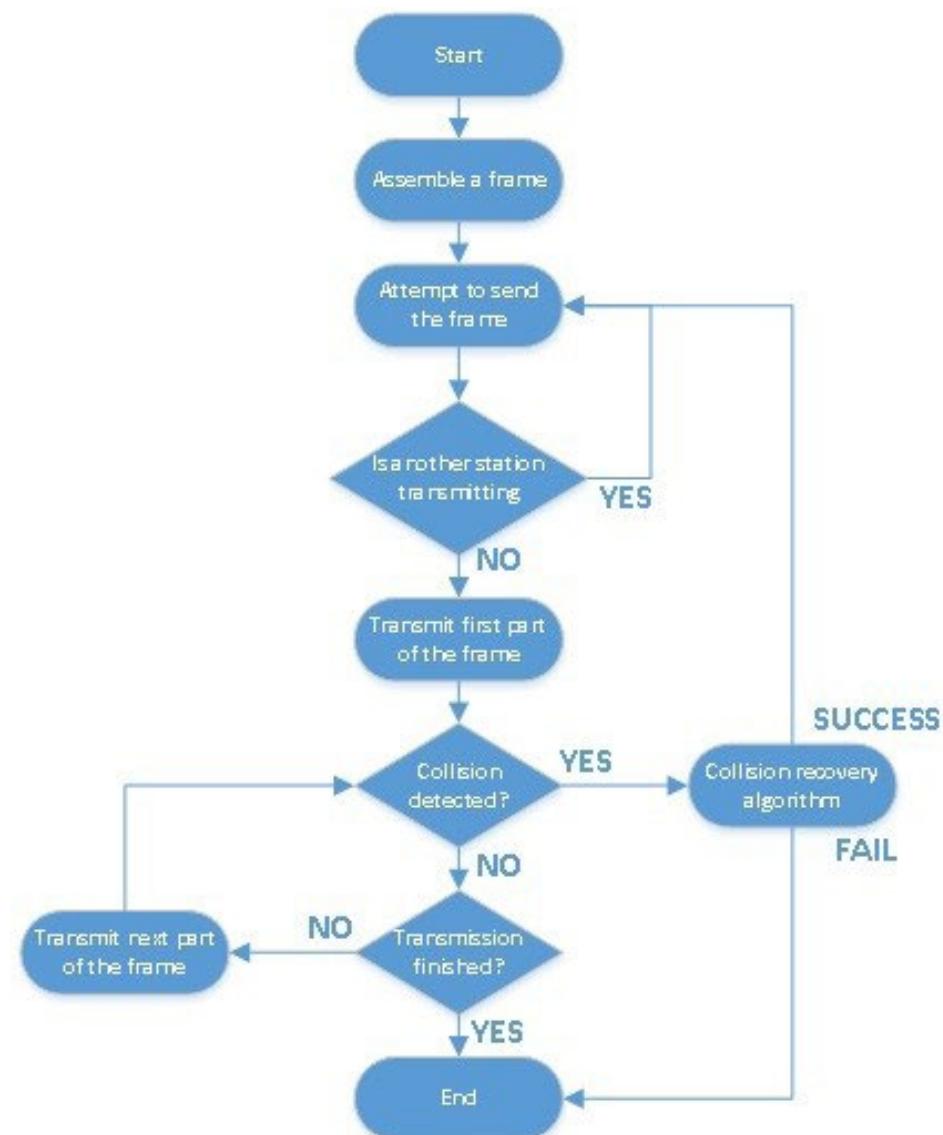
STP continues to monitor the network for redundant paths or links actively. If it finds them, it shuts them down immediately. STP ensures that the data is forwarded only through the active or approved path when data is forwarded.

# CSMA/CD

- Stands for Carrier Sense Multiple Access/Collision Detection (CSMA/CD)
- Is used for detecting collisions on a network
- Is device dependent
  - Device listens for traffic
  - Device transmits the traffic
  - Device stops transmitting if collision is detected

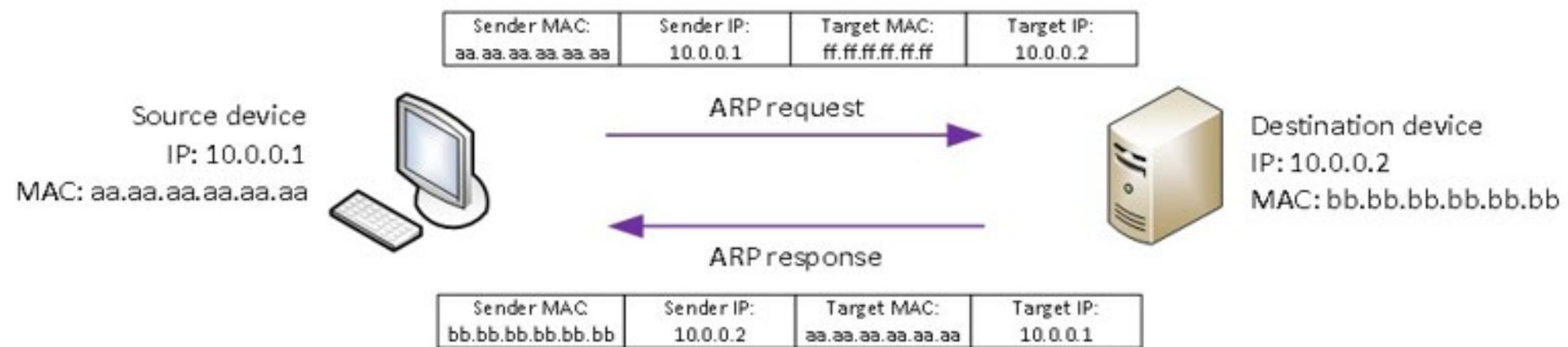
CSMA/CD stands for Carrier Sense Multiple Access with Collision Detection, used to detect collisions on a network. It is device-dependent as it needs to be enabled on the device. When a device has the CSMA/CD capability, it first listens to the traffic and then transmits it. If there is a collision taking place, the device stops transmitting the traffic.

With the CSMA/CD, a device is set to the listening mode, preventing the device from abruptly sending traffic. The device must first ensure that the network path or channel is clear to prevent a collision.



# Address Resolution Protocol (ARP)

- Resolves the IP address to MAC address
- Sends the MAC address to the source computer initiating a transfer
- Stores the MAC address with their IP addresses in the ARP cache
- Checks the ARP cache before sending out the packets on a network



# Address Resolution Protocol (ARP)

Arp stands for Address Resolution Protocol, which defines the mapping of an IP address to a MAC or the physical address of a network interface. You can use it to display the arp cache on a host. On Windows, you need to run the following command:

```
arp -a
```

On Linux, you can run the arp command to view the arp cache.

When a system needs to find the MAC address for an IP address, it adds the mapping to the ARP cache. This entry is used when next time the system needs to refer to the same MAC address. The arp command behaves slightly differently on Windows and Linux. If you execute it on Windows without any parameters, it lists the help information. However, on Linux, it displays the arp cache.

You can display all arp cache entries with the following command:

```
arp -a
```

You can also manipulate the arp cache. For example, you can delete an arp cache entry for a specific host with the following command:

```
arp -d localsystem
```

The -d parameter is the parameter, and the hostname, the localsystem, is the argument you need to pass to the arp command.

Using the -s parameter, you can also add a static arp entry:

```
arp -s 192.168.1.2 00-aa-00-62-c6-09
```

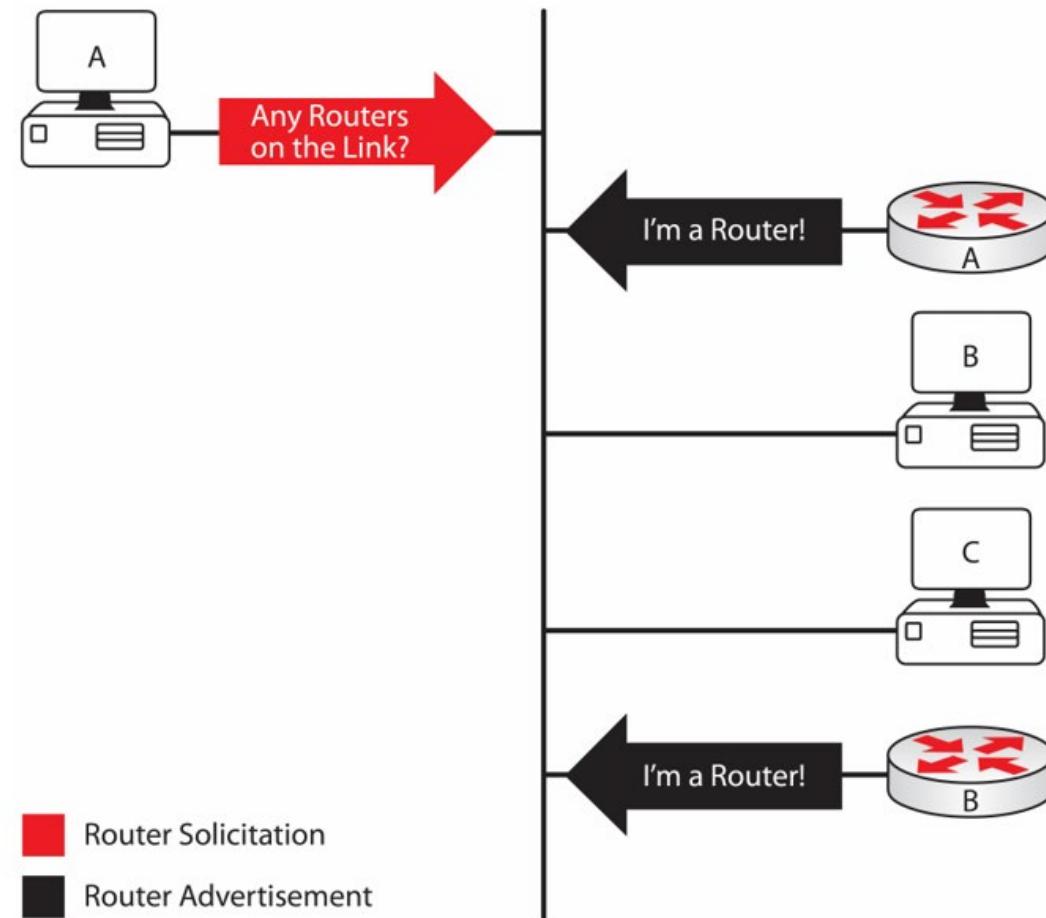
The ARP protocol plays an important role in communication over a network. When one device needs to find another device, it uses the IP address to track it. ARP uses the IP address to map it with the MAC address, which is stored in the ARP cache of the sending device. However, from here onwards, the MAC address is used for communication with the recipient device.

For example, device A wants to communicate with device B. It checks its ARP cache to find the MAC address of device B. If it is not found, then a discovery packet to get the MAC address of device B. After a response is received, it can then use the MAC address to communicate with device B.



# Neighbor Discovery Protocol

- Is used by IPv6 to determine the neighbors
- Works on the Link layer of the Internet network architecture
- Consists of Layer 1 (Physical) and Layer 2 (Data Link) of the OSI model
- Is used by the host router to find the neighboring routers
- Tracks an alternate path if the router to a path fails or is unreachable



# Neighbor Discovery Protocol

The Neighbor Discovery Protocol or NDP is mainly used in the IPv6 environment. It operates on the Link layer of the Internet network architecture. The Link layer maps to Layer 1 and Layer 2 of the OSI model. Layer 1 is the Physical layer, and Layer 2 is the Data Link layer.

The NDP protocol performs several tasks, such as:

Router solicitation

Router advertisement

Neighbor solicitation or advertisement

Address prefix discovery

It can perform other tasks such as duplicate address detection and address the discovery of the neighboring nodes on the link.

When a node is present on a link, it advertises its presence to every other active node. With this process, the node announces its presence and at the same time learns about the other active nodes that are present and active on the same link. After discovering the neighbours, a node can use them to forward its traffic to the required destination.

It also maintains a cache of the discovered nodes and their link-layer addresses. If the address of a router changes, the node updates its cache by overwriting its entry in the cache.

It often happens that the neighboring router fails or is inactive due to a specific reason. The node then finds an alternative to send out the traffic to its destination. This is done with the use of the NDP protocol.



# Summary

- Ethernet Switching Features



That's the end of the lesson.  
Here we covered:

- Ethernet Switching Features





**NEXT TOPIC**

---

# WIRELESS STANDARDS AND TECHNOLOGIES

---

Lesson

# 4

---

# Wireless Standards and Technologies

- 1 — Welcome to the lesson 4 of Module 2. In this lesson, you will learn about the:
  - 2 — Wireless Standards and Technologies
- 



Network Fundamentals

# AGENDA

- 802.11 Standards
- Frequencies and range
- Channels
- Channel Bonding
- Service Set Identifier (SSID)
- Antenna Types
- Encryption Standards
- Cellular Technologies
- Multiple input, multiple output (MIMO) and multi-user MIMO (MU-MIMO)



Hi, welcome to COMPTIA Network+ Course

In this lesson, we will talk about:

- 802.11 Standards
- Frequencies and range
- Channels
- Channel Bonding
- Service Set Identifier (SSID)
- Antenna Types
- Encryption Standards
- Cellular Technologies
- Multiple input, multiple output (MIMO) and multi-user MIMO (MU-MIMO)



A blurred background image of a person sitting at a desk, looking down at a laptop screen. The person is wearing a light-colored shirt and dark pants. The scene is softly lit, creating a professional yet approachable atmosphere.

*TOPIC 1*

---

# WIRELESS STANDARDS

---

# Wireless Standards

802.11ax

802.11ac

802.11n

802.11g

802.11b

In this section, you will learn about wireless standards. On the screen, you can see several wireless standards listed. The order is laid from bottom to top, which means , you will learn about 802.11a first and eventually end up with 802.11ax.



# 802.11a

802.11ax

802.11ac

802.11n

802.11g

802.11b

802.11a

- Speed: 5 GHz
- Max Data Rate: 54 Mbps
- Typical Indoor Range: 100 feet
- Typical Outdoor Range: 400 feet
- Topology: Ad-hoc, Infrastructure

Let's look at the first wireless standard, which is 802.11a. This standard uses the 5 GHz frequency and runs at 54 Mbps. Since it uses a 5 GHz frequency, it is compatible only with the wireless standards that operate simultaneously. For example, it is compatible with 802.11n because both of them operate at the same frequency. The 802.11a standard is not compatible with the standards that operate at 2.4 GHz. One such example is 802.11b which only operates at 2.4 GHz.

When you have a wireless network, its indoor range is typically less than the outdoor range. This is largely due to interferences and obstacles like walls or the building material that blocks the signal. Its typical indoor range is 100 feet, whereas, due to less interference, the outside range goes up to 400 feet.

The 802.11a wireless standard can work in ad-hoc or enterprise mode. The one you choose depends on your requirements. For example, at home, you would go with the ad-hoc mode. If you work in a decently sized organization, you are likely to set it up in the infrastructure mode.

# 802.11b

802.11ax

802.11ac

802.11n

802.11g

802.11b

802.11a

- Speed: 2.4 GHz
- Max Data Rate: 11 Mbps
- Typical Indoor Range: 150 feet
- Typical Outdoor Range: 450 feet
- Topology: Ad-hoc, Infrastructure

Let's look at the second wireless standard, which is 802.11b. This standard uses the 2.4 GHz frequency and runs at 11 Mbps. Since it uses a 2.4 GHz frequency, it is not compatible with the 802.11a wireless standard or any standard that operates at 5 GHz. For example, it is compatible with 802.11n because 802.11n operates at 2.4 and 5 GHz.

Its typical indoor range is 150 feet, whereas, due to less interference, the outside range goes up to 450 feet. In the wireless standards, the higher speed reduces the range. Since 802.11b has a lower speed, it offers a greater indoor and outdoor range.

The 802.11b wireless standard can work in ad-hoc or infrastructure mode.



# 802.11g

802.11ax

802.11ac

802.11n

802.11g

802.11b

802.11a

- Speed: 2.4 GHz
- Max Data Rate: 54 Mbps
- Typical Indoor Range: 150 feet
- Typical Outdoor Range: 450 feet
- Topology: Ad-hoc, Infrastructure

Let's look at the third wireless standard, which is 802.11g. This standard uses the 2.4 GHz frequency and runs at 54 Mbps, equivalent to the 802.11a standard. Since it uses a 2.4 GHz frequency, it is not compatible with the 802.11a wireless standard or any standard that operates at 5 GHz. For example, it is compatible with 802.11n and 802.11g because 802.11n operates at 2.4 and 5 GHz. One important point to note is that 802.11g is likely to have more interference from devices like a wireless keyboard, which also operates at 2.4 GHz.

Its typical indoor range is 150 feet whereas, the outside range goes up to 450 feet.

The 802.11g wireless standard can work in ad-hoc or infrastructure mode.



# 802.11n

802.11ax

802.11ac

802.11n

802.11g

802.11b

802.11a

- Speed: 2.4 / 5.0 GHz
- Max Data Rate: 600 Mbps
- Typical Indoor Range: 175 feet
- Typical Outdoor Range: 230 feet
- Topology: Ad-hoc, Infrastructure
- Backward Compatibility: 802.11a, 802.11b, and 802.11g

Let's look at the second wireless standard, which is 802.11b. This standard uses the 2.4 GHz frequency and runs at 11 Mbps. Since it uses a 2.4 GHz frequency, it is not compatible with the 802.11a wireless standard or any standard that operates at 5 GHz. For example, it is compatible with 802.11n because 802.11n operates at 2.4 and 5 GHz.

Its typical indoor range is 150 feet, whereas, due to less interference, the outside range goes up to 450 feet. In the wireless standards, the higher speed reduces the range. Since 802.11b has a lower speed, it offers a greater indoor and outdoor range.

The 802.11b wireless standard can work in ad-hoc or infrastructure mode.



# 802.11ac

802.11ax

802.11ac

- Speed: 5.0 GHz
- Max Data Rate: 1.3 Gbps
- Typical Indoor Range: 115 feet
- Typical Outdoor Range: -
- Topology: Ad-hoc, Infrastructure

802.11n

802.11g

802.11b

802.11a

The fifth wireless standard is 802.11ac, which is also known as Wi-Fi 5. The 802.11ac, just like 802.11a wireless standard, works only on the 5 GHz frequency. One of the major improvements in this wireless standard was speed. It could throttle up to 1300 Mbps (megabits per second) equivalent to 1.3 Gbps. Other than this, the 802.11ac standard also introduced Multi-User MIMO (MU-MIMO) and wide channels, which were now 80 or 160 MHz. Its predecessor, 802.11n, used 40 MHz channels.

The typical indoor range for 802.11ac is 115 feet, whereas the outdoor range is much larger, typically three times.

The 802.11b wireless standard can work in ad-hoc or infrastructure mode.



# 802.11ax

## 802.11ax

## 802.11ac

- Speed: 2.4 / 5.0 GHz
- Max Data Rate: 10-12 Gbps
- Typical Indoor Range: 150 feet
- Typical Outdoor Range: 300 feet
- Topology: Ad-hoc, Infrastructure

## 802.11n

## 802.11g

## 802.11b

## 802.11a

The 802.11ax is the latest standard in the wireless arena. It is also known as Wi-Fi6, which adds on the improvements over its predecessor, 802.11ac. The 802.11ax standard can operate in 2.4Ghz and 5Ghz frequency ranges.

The 802.11ax wireless standard offers a whopping speed of 10-12 Gbps and works within the indoor range of 150 feet. The outside range is 300 feet. The 802.11b wireless standard can work in ad-hoc or infrastructure mode.

The 802.11ax standard can support up to eight MU-MIMO transmissions.





*TOPIC 2*

---

# FREQUENCIES AND RANGE

---

# 2.4 vs. 5.0 GHz

	2.4 GHz	5.0 GHz
Supporting Standards	802.11 b/g/n/ax	802.11 a/n/ac/ax
Speed	450-600 Mbps	1300 Mbps
Coverage	150 Feet Indoor 300 Feet Outdoors	90 Feet indoor
Penetration Strength	Can penetrate through wood and concrete	Cannot penetrate through solid objects
Number of Channels	11	45
Channel Overlapping	Yes (All except 3 Channels – 1., 6, 11)	None
Interference	High	Low

On this slide, you can see a comparison of 2.4 and 5 GHz frequencies. Let's start with the supporting wireless standards. 2.4 GHz is supported by 802.11 b/g/n, whereas 5 GHz is supported by a/n/ac. 802.11n and 802.11ax are two standards that support both 2.4 and 5 GHz frequencies.

2.4 GHz, when compared with 5.0 GHz, has a lesser speed, which is between 450 to 600 Mbps. On the other hand, 5 GHz frequency can go up to 1300 MHz.

When you compare the coverage, it is obvious that the 5 GHz frequency has lesser coverage. The biggest reason is higher the speed, the lower the coverage. 2.4 GHz frequency can penetrate through solid objects, such as walls, which is a big shortcoming of 5 GHz frequency. It simply cannot penetrate through solid objects.

2.4 GHz frequency only has 11 channels, and only three channels, 1, 6, and 11, are non-overlapping channels. 5 GHz has only non-overlapping channels.

2.4 GHz is more susceptible to interference because several household appliances and electronic devices work on the same frequency. A cordless phone is a good example. 5 GHz is less prone to interference as compared to 2.4 GHz frequency.

A photograph of two people, a man and a woman, sitting at a table and looking at a laptop screen. The laptop displays a website with various images and text. The man is on the left, wearing a light-colored shirt, and the woman is on the right, wearing a dark top. They are both looking towards the laptop screen.

*TOPIC 3*

---

# CHANNELS

---

# Regulatory Impacts

Country	Number of Channels
USA	1-11
Europe	1-13
Japan	1-1

Most countries in the world have their regulations to regulate wireless transmissions. It is also common for the adjoining countries to use the same regulations. For example, the table on the slide lists some countries with regulated standards to use a specific number of channels.



*TOPIC 4*

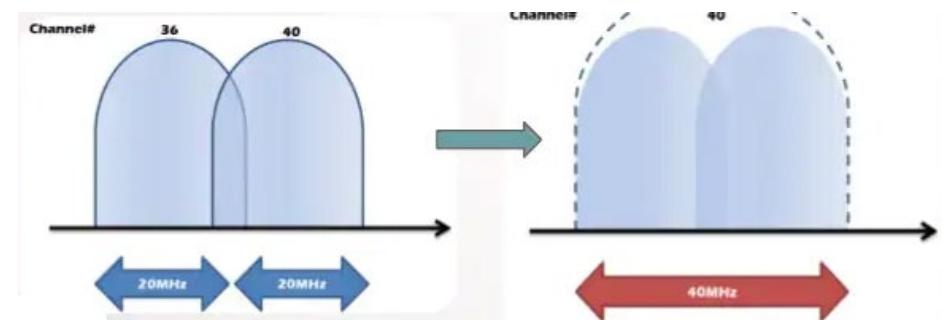
---

# CHANNEL BONDING

---

# Channel Bonding

- Combines different channels to increase the throughput
- Was introduced in 802.11n
- Is configured with channels 1 and 6 in 2.4 GHz range
  - Has total width of 70 MHz
  - Forms a channel of 40 MHz (20 + 20)
  - Leaves a single non-overlapping channel, 11 with 30 MHz
- Can be configured with 5.0 GHz
  - Has a total width of 500 MHz
  - Allows multiple bonded channels because they are non-overlapping



<https://www.slideshare.net/GiorgosFragiadakis/channel-bonding>

Channel bonding is a method of combining two non-overlapping channels to get better throughput. If a single channel has a specific throughput, you can combine another non-overlapping channel with the same throughput.

The concept of channel bonding was introduced in the 802.11n wireless standard. The pre-requisites are that the channels must be non-overlapping and must have the same throughput. In 2.4 GHz frequency, you have channels 1, 6, and 11 as the non-overlapping channels. For example, you can configure channel bonding with 1 and 6.

All three channels, 1, 6, and 11, have a combined width of 70 MHz. Both channels, 1 and 6, have a core frequency of 20 MHz. When you combine both the channels, you get a width of 40 MHz, combining 20 and 20. You can label this channel as either 1 or 6. On the other hand, this leaves channel 11 alone with the 30 MHz width.

When you refer to the 5 GHz frequency, there are 25 non-overlapping channels, which have an aggregated width of 500 MHz. With the 25 non-overlapping channels, you can create several pairs of bonded channels.

## **TOPIC 5**

---

# **SERVICE SET IDENTIFIER (SSID)**

---



# Basic Service Set

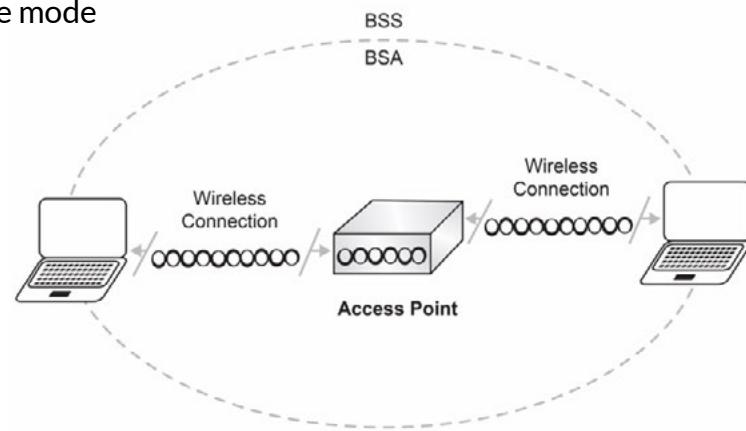
## Basic Service Set

- Is a name given to the logical WLAN segment
- Contains only one wireless access point (WAP)
- Does not support mobility as there is a single WAP
- Is also known as the infrastructure mode

## Extended Service Set

## Independent basic service set (Ad-hoc)

## Roaming



Basic Service Set is the name given to the logical WLAN segment that contains a single wireless access point (WAP). You may have several wireless clients in an organization or at home, ranging from laptops, mobiles, televisions, or tablets. Each one of them connects to a single WAP. The wireless clients must authenticate themselves with the WAP using a designated authentication method. After the clients are authenticated, they can communicate with each other on a single logical WLAN segment. Since the WAP is connected to the wired network or a physical network cable, if clients are on the wired network, the wireless clients can communicate with them.

One of the big disadvantages of this mode is that it does not offer mobility to wireless clients as there is a single WAP. Another disadvantage is that the WAP can broadcast signals only to a limited area, and if the wireless clients are present outside that area, they cannot connect with the WAP.

The Basic Service Set is also known as infrastructure mode, as it requires a centralized WAP for the wireless clients to connect.

# Extended Service Set

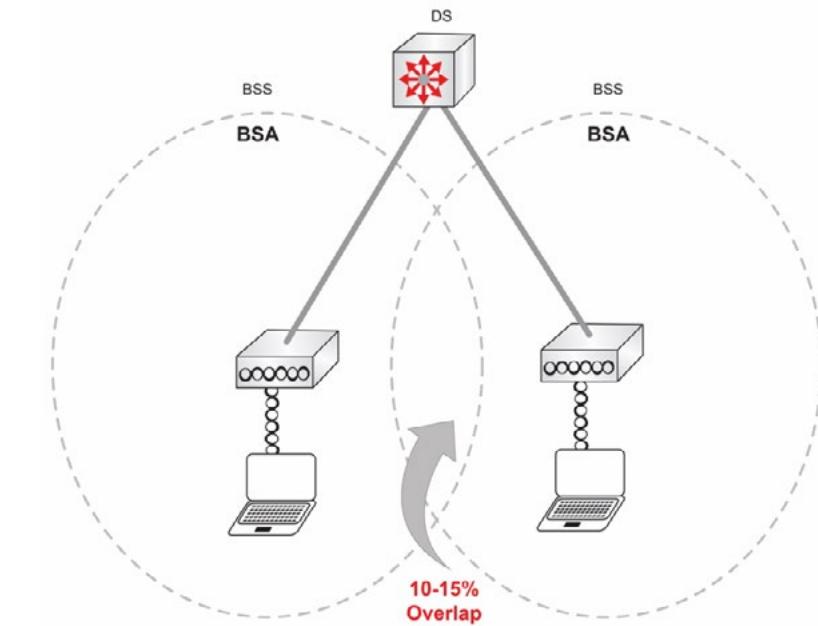
Basic Service Set

Extended Service Set

Independent basic service set (Ad-hoc)

Roaming

- Connects more than one WAPs
- Allows clients to move from one WAP to another WAP
- Requires each WAP to use the same SSID
- Allows the WAPs to have unique BSSID



Extended Service Set is an extension of Basic Service Set, which had a limitation of a single WAP. In the Extended Service Set, there are more than one WAPs, each one having the same SSID. When a wireless client authenticates with one of the WAPs, it can roam around the facility or building. As the wireless client moves out of the range of the first WAP and comes into the second one, it is disassociated from the first WAP and joined with the second WAP automatically. The entire process to the wireless client is transparent.

In Extended Service Set, even though the WAPs need to have the same SSIDs, they can have different BSSIDs, which is the name of the WAP. To set up an Extended Service Set, you need to have more than one Basic Service Sets, which are then combined. Eventually, you end up covering a large area.

For example, if you ever connected to the free wireless network at an airport. You can roam around from one location to another location without being disconnected. In reality, you have connected to the Extended Service Set.

In the given diagram, you have an Extended Service Set with two Basic Service Sets, my wifi. When a wireless client moves from one Basic Service Set to another one, there is no disconnection. It is just a handoff from one WAP to another WAP.

# Independent Basic Service Set (Ad-hoc)

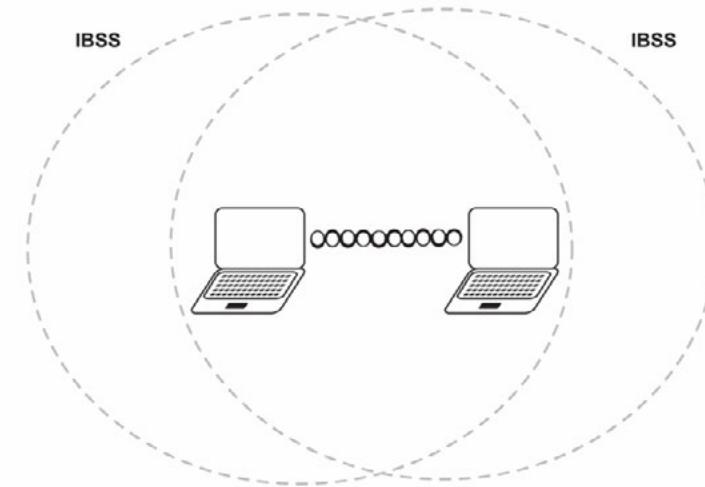
Basic Service Set

Extended Service Set

Independent basic service set (Ad-hoc)

Roaming

- Is also known as the Ad-hoc mode or peer-to-peer network
- Is a simple wireless network that allows the wireless clients to communicate with each other
- Does not require a router or WAP in between to connect with the clients



Independent Basic Service Set is also known as Ad-hoc or peer-to-peer wireless network, a direct connection between two wireless clients. Let's take the example of two mobile phones connecting using Bluetooth. You may have to transfer files from one mobile to another mobile while sitting in a park. This is the most appropriate wireless network you can form.

When they connect, they form an ad-hoc network. Unlike the Basic Service Set or Extended Service Set, there is no centralized WAP between two clients.

It is important to know that an ad-hoc network can also be configured on a wireless router. Once this is set up, the wireless clients can communicate with each other without involving the wireless router.

# Roaming

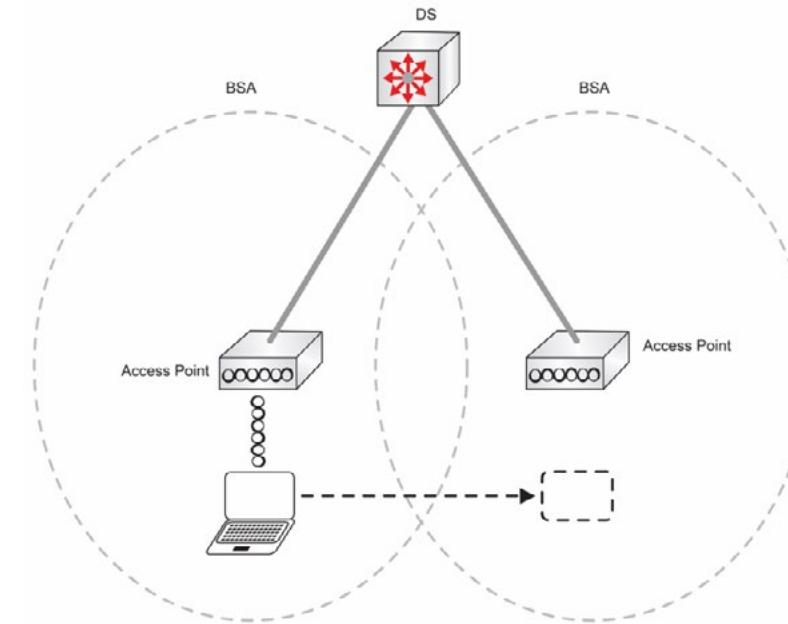
Basic Service Set

Extended Service Set

Independent basic service set (Ad-hoc)

Roaming

- Allows the clients to move from one WAP to another WAP
  - Keeps a persistent connection
  - Does not require re-authentication with the second WAP
- Requires the WAPs to be configured with same SSIDs



# Roaming

A few slides back, you learned about the Extended Service Set, which allowed the wireless clients to move from one WAP to another without getting disconnected. One of the pre-requisites for the WAPs to work in the Extended Service Set was to have the same SSID.

When a wireless client moves from one WAP to another WAP, it is called roaming. The wireless clients keep a persistent connection without getting disconnected or re-authenticating themselves with the second WAP. When a wireless client is moving from one WAP to another WAP, a complete handoff process is executed. This process involves three steps: scanning, authentication, and association.

Let's look at these steps.

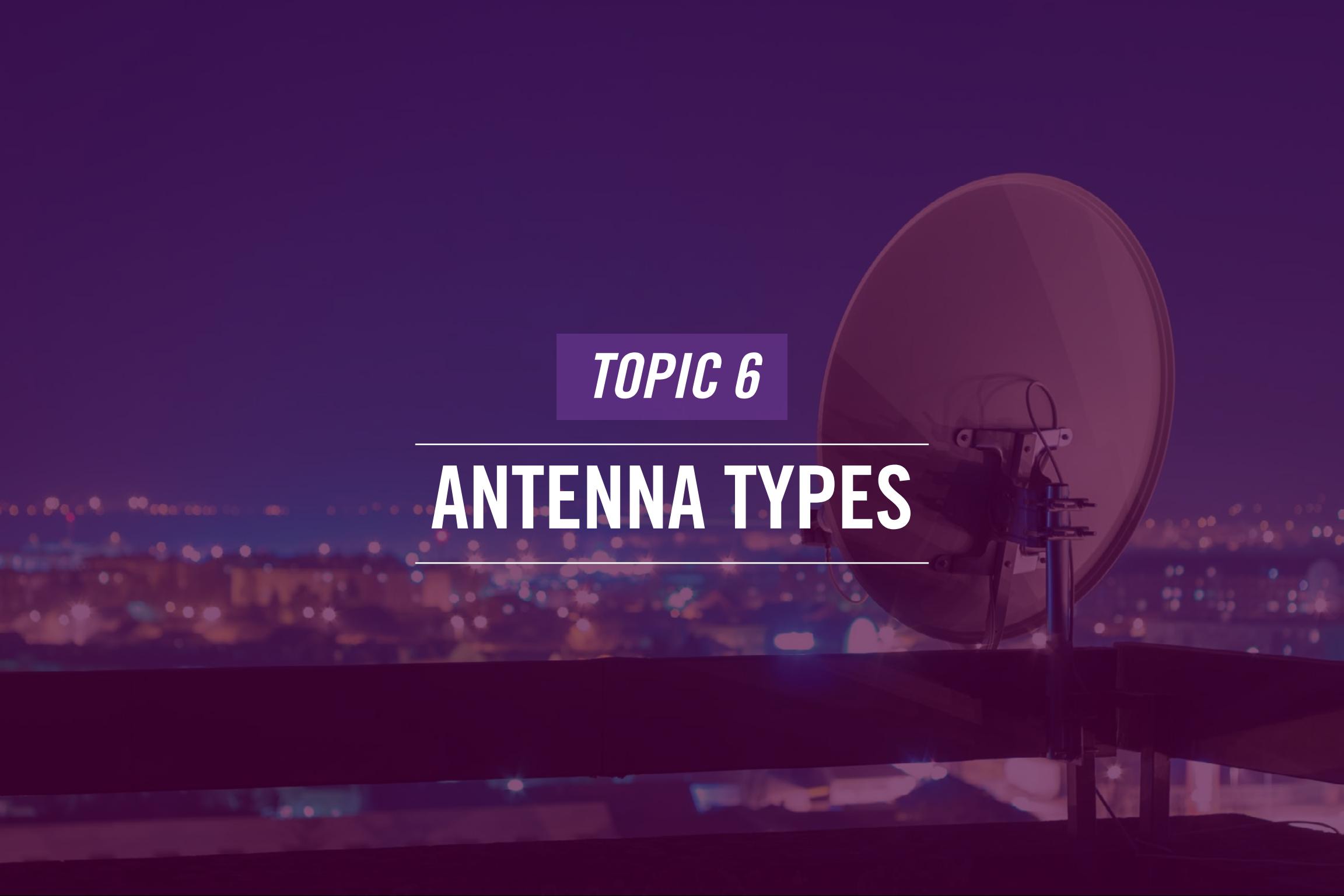
1. Scanning: When a wireless client moves away from the currently connected WAP, it attempts to find a new WAP. When it locates the new WAP with the same SSID, it sends an authentication request to the WAP.

2. Authentication: After receiving the wireless client's authentication request, the WAP authenticates it after verifying its credentials.

3. Association: As the wireless client is authenticated, it sends an association request to the new WAP, finally accepting the association request. After accepting the association request, the new WAP sends a disassociation request to the old WAP to dissociate the wireless client. After receiving the request, the old WAP dissociates the wireless client. After the association with the wireless client, the new WAP updates its routing tables.

Even though this seems like a lengthy process, it happens in a split of a second. The entire process is transparent to the end-user who is using the wireless client.



The background of the slide features a large satellite dish antenna mounted on a metal pole. The dish is positioned on the right side of the frame, pointing towards the left. The background is a dark, out-of-focus view of a city at night, with numerous small lights visible.

## *TOPIC 6*

---

# ANTENNA TYPES

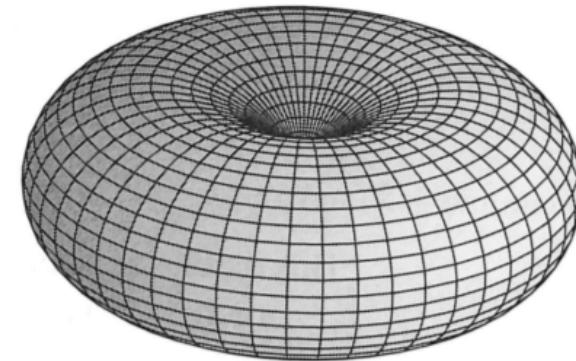
---

# Omni

## Omni

## Directional

- Transmit signals to all directions equally
- Are used in wireless routers, mobiles, and radio transmission towers
- Are easy to install and implement
- Can be installed in any direction
- Have shorter range as signal is transmitted in all directions



**Figure 14.21 – Omnidirectional Antenna Radiation Pattern**  
(Image Introduction to Electrodynamics, by D. Griffiths, 4th Ed.)

Antennas are essential of two types: Omni-directional and directional. Let's first start with the Omni-directional, which can transmit signals in all directions equally. For example, if a device, such as a wireless router, is placed in the middle of a room, it will transmit the signals with equal strength to all corners. You would have used Omni-directional antennas in several devices, such as wireless routers, cell phone antennas, and radio transmission towers – all of them transmit signals in all directions equally.

The key advantage of Omni-directional antennas is that they are easy to install. You can place them in any direction or location in a room. You will still get the signals in all corners of the room.

The key disadvantage of Omni-directional antennas is that they have a shorter range as they transmit the signals in all directions. Since the signals are spread out, they reach only a certain distance.

# Directional

Omni

Directional

- Transmit narrow directional signals
- Are used when you need signals in a specific direction, such as television antennas
- Have good transmission and reception of signals



[www.lairdconnect.com](http://www.lairdconnect.com)

The second type of antenna is a directional antenna, which sends signals in a specific direction. Unlike Omni-directional antennas, these antennas are designed to focus on a specific direction. The focus is on a single direction with good strength of signals. The interference is also reduced. The strength of signals overrides the interference in this case.

As the signal strength in a specific direction is an advantage, broader coverage becomes a disadvantage. You cannot cover all corners with signals.

A good example is a satellite dish that receives and transmits signals from a specific direction.

## *TOPIC 7*

---

# ENCRYPTION STANDARDS

---

# WPA2 Personal

WPA2 Personal

- Uses the pre-shared keys (PSKs)
- Is deployed at home or smaller offices
- Uses AES-CCMP for data encryption

WPA2 Enterprise

The screenshot shows a configuration page for a TP-Link router's wireless settings. The top section is titled "WPA-PSK/WPA2-PSK". It contains three dropdown menus: "Version" set to "WPA2-PSK", "Encryption" set to "AES", and a "PSK Password" field containing "TestTPLINK". A red box highlights these three fields. Below them is a note: "(You can enter ASCII characters between 8 and 63 or Hexadecimal characters between 8 and 40)." Underneath is a "Group Key Update Period" field with a value of "0" and a note: "(in second, minimum is 30, 0 means no update)". At the bottom is a "Save" button.

<https://www.tp-link.com/>

After WEP and WPA, WPA2 is the latest security protocol that is in use. It is found in all wireless routers, designed to be used at homes or in large enterprises. The WPA2 protocol comes in two different versions: Personal and Enterprise. Let's first start with the WPA2 Personal.

It uses a pre-shared key, a secret known by the wireless router and the wireless client. WPA2 Personal is mostly used at home or in a small office with no centralized authority to authenticate wireless clients. WPA Personal uses AES-CCMP to encrypt data in transmission over the wireless network.

# WPA2 Enterprise

WPA2 Personal

WPA2 Enterprise

- Is mainly used in an enterprise environment
- Requires a RADIUS server for authenticating users
- Uses Counter Cipher Mode with Block-Chaining Message Authentication Code Protocol (CCMP) and Advanced Encryption Standard (AES) algorithms

The screenshot shows a 'Security Settings' dialog box. At the top, it says 'Select SSID: SSIDName1'. Below that, 'Security Mode:' is set to 'WPA2-Enterprise', which is circled in red. The 'Encryption:' field is set to 'AES'. The 'RADIUS Server:' field contains '0 . 0 . 0 . 0' with a note '(Hint: 192.168.1.200)'. The 'RADIUS Port:' field is set to '1812' with a note '(Range: 1 - 65535, Default: 1812)'. The 'Shared Key:' field is empty and redacted. The 'Key Renewal:' field is set to '3600' with a note '(Range: 600 - 7200, Default: 3600)'. At the bottom are three buttons: 'Save', 'Cancel', and 'Back'.

<https://www.techjunkie.com/>

WPA2 Enterprise, as the name suggests, is used in enterprises or large organizations. However, it is not necessary that WPA2 Personal must be used only at home or in small organizations. It can also be used in large enterprises. However, it is not a secure option to be used with enterprises.

With the Enterprise method, you need to use a RADIUS server, which performs the authentication. Unlike Personal, the Enterprise method does not rely on shared passwords, which eventually removes another risk of passwords being sniffed. Whereas Personal uses PSKs or pre-shared keys, the WPA2 Enterprise uses the IEEE 802.1X method, a network authentication protocol for protected authentication.

Just like WPA2 Personal, Enterprise also uses AES-CCMP for data encryption during transmission.



The background features a complex, abstract network visualization. It consists of numerous small, glowing blue and orange dots representing data points or nodes, connected by a web of thin, light-colored lines forming a mesh-like structure. Some nodes are larger and more prominent, suggesting they are central to the network. The overall effect is one of a dynamic, interconnected system.

*TOPIC 8*

---

# CELLULAR TECHNOLOGIES

---

# CDMA

CDMA

GSM

LTE

3G, 4G, 5G

- Stands for Code Division Multiple Access
- Stores the information in the handset
- Was used in 2G and 3G communications
- Has limited roaming capabilities
- Uses 800 MHz and 1900 MHz frequencies

CDMA stands for Code Division Multiple Access. CDMA is a handset-specific technology, which means that it does not require a SIM card. Rather, it uses codes to identify the caller. The mobile number is hard-coded into the mobile. For example, if there is an issue with the number, you will have to replace the handset. CDMA uses the 800 and 1900 MHz frequencies.

CDMA, at one point, was a popular technology and was mainly used in 2G and 3G communications. However, across the world, the number of CDMA users has reduced drastically. It is mostly being used in the USA, Canada, and Japan. Because of its less support by the service provider, a CDMA user has limited roaming capabilities.

CDMA uses the 800 and 1900 MHz frequencies and uses 1xEV-DO (EVDO or Evolution Data Optimization), the 3G standard for CDMA networks. One of the key advantages of CDMA is that it has built-in encryption. However, one of its main disadvantages was that it could not send voice and data simultaneously.



# GSM

CDMA

GSM

LTE

3G, 4G, 5G

- Stands for Global System for Mobile Communications
- Uses one of the two frequencies:
  - 900 MHz
  - 1800 MHz
- Digitizes and compresses data before sending it out using a channel
- Identifies callers using:
  - Frequency Division Multiple Access (FDMA)
  - Time Division Multiple Access (TDMA)

GSM stands for Global System for Mobile Communications, which can be used for voice calls and data. GSM is designed to use two frequency bands, which are 900 and 1800 MHz. The 900 MHz band is known as GSM-900. The 1800 MHz band is known as DCS-1800. Before sending out the information, LTE first digitizes the information and then compresses it, allowing it to send a smaller amount of information in a much faster way.

GSM uses the physical and logical channels for processing information.

GSM identifies callers using Frequency Division Multiple Access (FDMA) and Time Division Multiple Access (TDMA).



# LTE

CDMA

GSM

LTE

3G, 4G, 5G

- Stands for Long-term Evolution
- Uses the Orthogonal Frequency Division Multiplexing (OFDM) for data transmission
- Uses frequencies to create multiple channels
- Uses three different channels to process information:
  - Physical
  - Logical
  - Transport

LTE stands for Long-Term Evolution that was invented and then used for high-speed data transmissions. LTE is designed to use Orthogonal Frequency Division Multiplexing (OFDM) for data transmission.

LTE works with two sets of bands, which are

- Frequency bands 1-25: These bands are reserved for Frequency Division Duplex (FDD)
- Frequency bands 33-41: These bands are reserved for Time Division Duplex (TDD)

When processing information, LTE, unlike GSM that uses two channels, uses three channels, namely physical, logical, and transport.



# 3G, 4G, 5G

CDMA

GSM

LTE

3G, 4G, 5G

	3G	4G	5G
Bandwidth	2 Mbps – 21 Mbps	100 Mbps – 1 Gbps	>1 Gbps
Type of Internet Services Used	Broadband	Ultra Broadband	Wireless World Wide Web
Use Cases Examples	Video Conferencing, Mobile TV, Global Positioning System (GPS)	High-speed applications, mobile TV, and wearable devices	High-resolution video streaming, robots, remote-controlled devices

Each generation of mobile networks brings something new, which is an obvious improvement over the previous version. For example, speed is an obvious improvement over the previous version. When you talk about 3G, it had a maximum speed of 21 Mbps, but 4G could go up to 1 Gbps.

The table on the slide explains the speeds, type of Internet Services used by each generation and their use cases.



*TOPIC 9*

---

# MIMO AND MU-MIMO

---

# MIMO

MIMO

MU-MIMO

- Stands for Multiple Input Multiple Output
- Used by 802.11n and 802.11ac
- Process:
  - The sender router breaks the signals into multiple streams using different antennas
  - The recipient router recombines the streams back to the original signal
- Can serve one device at a time

MIMO stands for Multiple Input Multiple Output, initially introduced in the 802.11n standard and then carried over to 802.11ac. MIMO is also known as Single User MIMO or SU-MIMO. MIMO uses a method called spatial multiplexing in which the sender wireless router breaks an outgoing signal into multiple streams and sends them out using different antennas. When these streams reach the recipient wireless router, it recombines the streams back into the original signal.

For MIMO to work, both the sender and recipient need to have this feature or the capability. MIMO is capable of serving one device at a time. However, this does not indicate that you cannot have multiple devices connected. They can be connected, but they will have to take turns. The communication with each device connected cannot happen simultaneously. When the communication is taking place with one device, the other devices have to wait.



# MU-MIMO

MIMO

MU-MIMO

- Stands for Multi-User MIMO
- Is an advanced version of MIMO
- Can send signals to more than one device at a time
- Was introduced in 802.11ac wireless standard
  - Only downlink with 802.11ac
  - Both downlink and uplink with 802.11ax
- Works only with 5 MHz frequency

MU-MIMO is a Multi-User MIMO, which is an enhancement of SU-MIMO even though it is backward compatible. It offers a major enhancement, which is that it can communicate with more than one device simultaneously. This was the shortcoming in MIMO. MU-MIMO used several forms of multiplexing that enabled it to communicate with multiple devices simultaneously.

MU-MIMO was introduced in 802.11ac, but it could work with the downlink connections. The latest wireless standard, 802.11ax, now works with an enhancement in MU-MIMO that supports downlink and uplink connections. It is important to note that MU-MIMO does not support 2.4 GHz and works only with a 5 GHz frequency.



# Summary

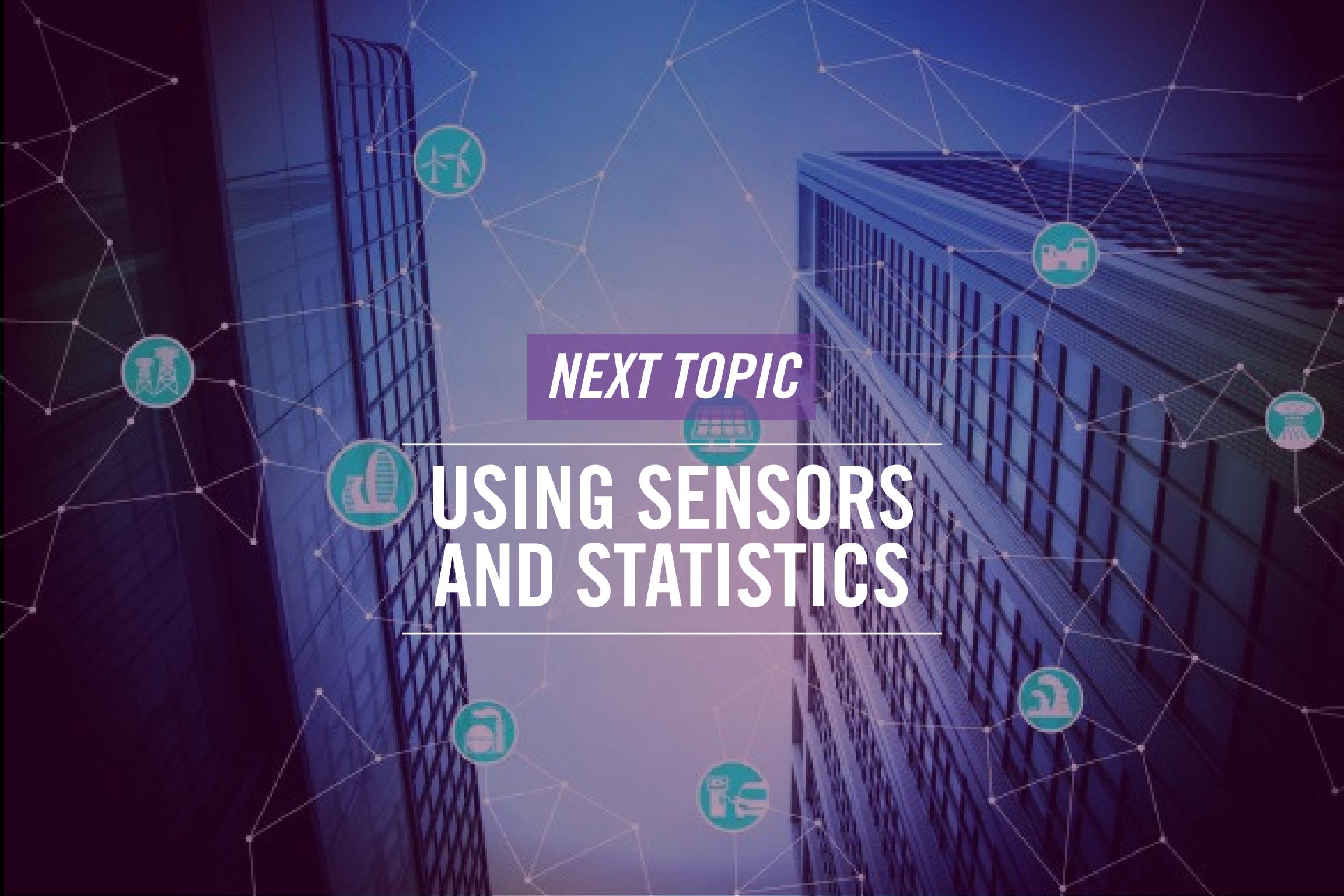
- 802.11 Standards
- Frequencies and range
- Channels
- Channel Bonding
- Service Set Identifier (SSID)
- Antenna Types
- Encryption Standards
- Cellular Technologies
- Multiple input, multiple output (MIMO) and multi-user MIMO (MU-MIMO)



That's the end of the lesson.

Here we covered:

- 802.11 Standards
- Frequencies and range
- Channels
- Channel Bonding
- Service Set Identifier (SSID)
- Antenna Types
- Encryption Standards
- Cellular Technologies
- Multiple input, multiple output (MIMO) and multi-user MIMO (MU-MIMO)



*NEXT TOPIC*

# USING SENSORS AND STATISTICS

---

# MODULE 3

---

# Module 3

LESSON 1 [USING SENSORS AND STATISTICS](#)

LESSON 2 [ORGANIZATIONAL DOCUMENTS AND POLICIES](#)

LESSON 3 [HIGH AVAILABILITY AND DISASTER RECOVERY](#)



Lesson

1

---

# Using Sensors & Statistics

- 1 — Welcome to the first lesson of Module 3. In this lesson, you will learn about the:
  - 2 — Using Sensors And Statistics
- 



Network Fundamentals

# Agenda

- Performance Metrics/Sensors
- SNMP
- Network Device Logs
- Interface Statistics/Status
- Interface Errors or Alerts
- Environmental Factors and Sensors
- Baselines
- NetFlow Data
- Uptime/Downtime

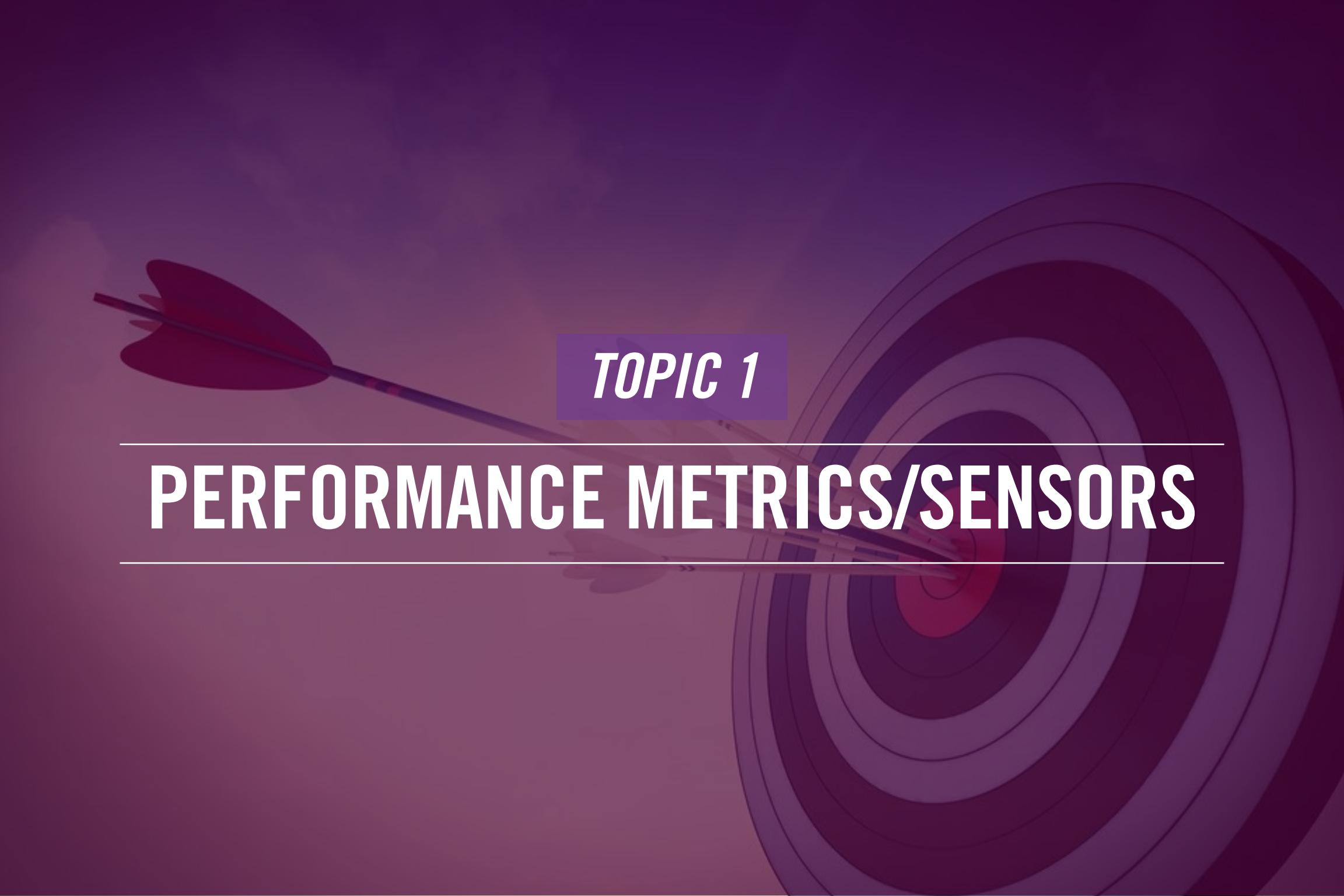


Hi, welcome to COMPTIA Network+ Course

In this lesson, we will talk about:

- Performance Metrics/Sensors
- SNMP
- Network Device Logs
- Interface Statistics/Status
- Interface Errors or Alerts
- Environmental Factors and Sensors
- Baselines
- NetFlow Data
- Uptime/Downtime



The background features a large, stylized target on the right side, with concentric circles in shades of purple and red. A single dart with a dark red feather hits the exact center of the bullseye. The rest of the slide is a solid dark purple color.

## *TOPIC 1*

---

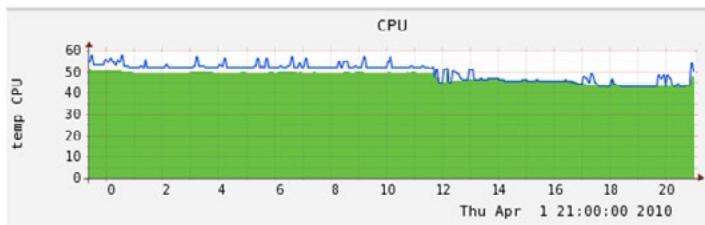
# PERFORMANCE METRICS/SENSORS

---

# Performance Metrics/Sensors – Device/Chassis

Network Metrics

Device/Chassis



- Temperature
  - Larger devices generate more heat
  - Heat causes damages and reboots to the devices
  - Heat can be pulled in from outside
  - Optimum temperature: 60°F to 90°F
- Central Processing Unit (CPU) usage
  - Is monitored with performance counters
  - Can use different performance counters depending on a role
- Memory
  - Requirement is dependent on a server role
  - Can be monitored by different performance counters

# Performance Metrics/Sensors – Device/Chassis

All network devices, servers, and systems produce heat. The larger the device or a server, the more heat it is going to generate. Compare a large server with a smaller server –the larger server will produce more heat. In a data center, you will find hundreds and thousands of such large servers. You can use multiple the amount of heat from these servers.

The amount of heat that is generated is dangerous for the devices and servers in a data center. If appropriate ventilation is not designed or heating is not handled properly, it can cause damage to the devices and servers. The heat is absorbed by the devices from outside and damages the devices. The heat is usually trapped inside a system or server because of a bad fan or clogged ports. On top of it, the system is also absorbing external heat. All this put together can malfunction the device or reboot it to ensure it cools down. To ensure that heat is always under control, you must keep the datacenter temperature between 60°F to 90°F.

A CPU is the heart of a device, system, or server. It needs to function properly and provide optimum performance. To ensure that it does, you can monitor the CPU using several performance counters. For example, you can use the Processor\% User Time performance counter that measures the time a CPU spends in the user mode, which is about working on an application. The performance counters should measure the current status against the defined baseline, representing the optimum performance threshold.

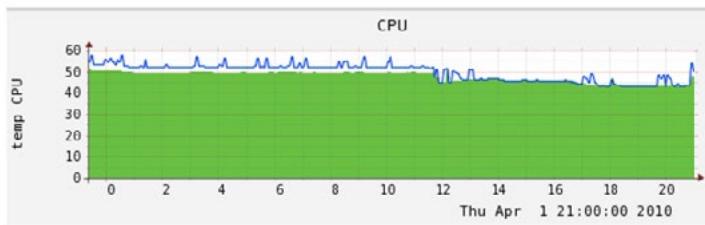
A server can be configured with different roles. For example, it could be a file server or a Webserver. You need to use the appropriate performance counters to measure the server in that specific role.

When it comes to memory, each application running on a server has a different requirement. Let's say that one application requires 2 gigabytes to function. The operating system requires a minimum of 4 gigabytes. To measure the memory performance, just like CPU, you can use several performance counters, such as Memory\% Committed Bytes in Use, which measures the total virtual memory in use. This way, you can calculate the total requirement for memory in a particular system.

# Performance Metrics/Sensors – Network Metric

## Network Metrics

## Device/Chassis



- Network Bandwidth:
  - Requirements depend on the applications being used
  - Should be monitored using performance counters, such as Network Interface\Output Queue Length
- Latency:
  - Is the time it takes for a packet to reach the destination from a source
  - Can be impacted by applications, specifically security auditing
- Jitter:
  - Is the delay in sending packets over a network connection
  - Can occur due to various reasons, such as route changes and network congestion

# Performance Metrics/Sensors – Network Metric

It is also critical to monitor the network performance. Several factors must be considered for optimal performance. For example, what is network bandwidth utilization? Each network has a certain amount of bandwidth. In most cases, organizations suffer from bandwidth congestion because users download or upload large files, applications eat up bandwidth, or unwanted traffic flows over the network. There can be several reasons.

To use the network bandwidth optimally, you need to start monitoring it. You need to define the threshold, known as a baseline, for normal utilization. Then, when you monitor it, you can determine the deviation from the standard usage. To monitor the network bandwidth, you can use several performance counters. For example, you can use the Network Interface\Bytes Total/Sec performance counter to measure the percentage of bandwidth a network interface uses against its total capacity. If the usage is more than 70 percent, then you know that the network interface is overloaded.

Latency is the time that a packet takes to reach its destination. The higher the time it takes, the more latency is there in the network. Generally, the latency is low on an internal network. However, when a packet leaves a network to a remote destination on the Internet, it faces latency challenges.

On an internal network, the latency can be added by using several applications like security applications. If there are traffic filtering rules added on a router, it can add to the latency. You can measure the latency with the use of the ping command.

Jitter is the inconsistency in latency. It is the delay in sending packets over a network. For example, if a packet from Device1 takes one millisecond to reach Device2, there is no jitter. Next time, it takes three milliseconds, and the third time, it takes two milliseconds. So, there are differences in timing every time you send a packet. This is the variation in latency, which you can jitter.



A photograph showing a person's hands holding a tablet. The tablet screen displays a complex dashboard with multiple graphs, charts, and data tables, likely representing network monitoring or system performance. The hands are positioned as if the person is interacting with the device. The tablet is placed on a light-colored wooden surface. To the right of the tablet, there is a white cup and saucer containing a dark liquid, possibly coffee or tea. The overall scene suggests a professional or technical environment where data analysis is taking place.

***TOPIC 2***

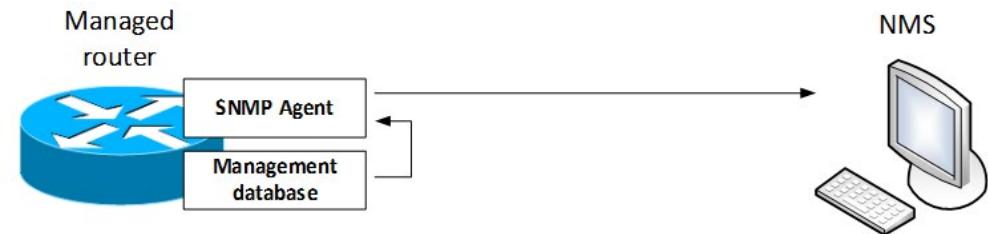
---

# SNMP

---

# SNMP

- Is a protocol that is used for:
  - Identifying devices on a network
  - Tracking network changes
  - Monitoring the network performance
  - Obtaining the device status
- Uses the client/server architecture with managers and agents
- Contains the following in the hierarchy:
  - Management Information Bases (MIBs) for storing information in hierarchical format
  - Object Identifiers (OIDs) to monitor devices and their status
  - Traps send information from the devices to the Managers



A network has several devices and systems. They need to be monitored for their availability. Sometimes, it becomes difficult even to track these devices on the network. If a network device goes down or becomes unavailable, it is not easy to track them. The Simple Network Management Protocol, or SNMP, is the solution that meets all these requirements. SNMP helps you by:

- Identifying devices on a network – what type of device it is
- Tracking network changes – new devices are added, or older ones are removed
- Monitoring the network performance – health of the network
- Obtaining the device status – whether the device is functional or not

If SNMP is not used, then there is no way to perform the tasks mentioned above efficiently.

SNMP works with the client/server architecture where the managers and agents are the clients. The managers collate the information from the agents that are installed on the various network devices. It could be a server, a switch, or a router. The agents send the device information to the managers.

SNMP works in a hierarchical manner that contains:

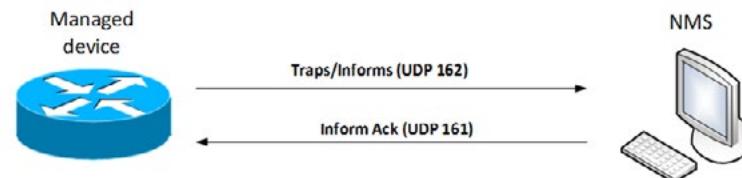
- Management Information Bases (MIBs) for storing information in a hierarchical format. Each agent has a local MIB from which it sends the information to the managers.
- Object Identifiers (OIDs) are unique to each device being monitored. It is used to describe the state of the device.
- Traps to send information from the devices to the Managers

# SNMP

The three versions of SNMP are versions 1, 2, and 3. Version 1, or SNMPv1, is the initial implementation of the SNMP protocol. SNMPv1 operates over protocols such as User Datagram Protocol (UDP), Internet Protocol (IP), and the OSI Connectionless Network Service (CLNS). SNMPv1 is widely used and is the de facto network-management protocol used within the Internet community.

SNMPv2 revises SNMPv1 and includes improvements in the areas of performance, security, confidentiality, and manager-to-manager communications. SNMPv2 also defines two new operations:

- GetBulk
- Inform



A network has several devices and systems. They need to be monitored for their availability. Sometimes, it becomes difficult even to track these devices on the network. If a network device goes down or becomes unavailable, it is not easy to track them. The Simple Network Management Protocol, or SNMP, is the solution that meets all these requirements. SNMP helps you by:

- Identifying devices on a network – what type of device it is
- Tracking network changes – new devices are added, or older ones are removed
- Monitoring the network performance – health of the network
- Obtaining the device status – whether the device is functional or not

If SNMP is not used, then there is no way to perform the tasks mentioned above efficiently.

SNMP works with the client/server architecture where the managers and agents are the clients. The managers collate the information from the agents that are installed on the various network devices. It could be a server, a switch, or a router. The agents send the device information to the managers.

SNMP works in a hierarchical manner that contains:

- Management Information Bases (MIBs) for storing information in a hierarchical format. Each agent has a local MIB from which it sends the information to the managers.
- Object Identifiers (OIDs) are unique to each device being monitored. It is used to describe the state of the device.
- Traps to send information from the devices to the Managers

# SNMP

The GetBulk operation is used to retrieve large blocks of data efficiently. The Inform operation allows one NMS to send trap information to another NMS and then to receive a response. In SNMPv2, if the agent responding to GetBulk operations cannot provide values for all the variables in a list, then it provides partial results. SNMPv3 provides the following three additional security services that are not available in previous versions of SNMP:

- Message integrity
- Authentication
- Encryption

SNMPv3 uses message integrity to ensure that a packet has not been tampered with in-transit. SNMPv3 also utilizes authentication, which is used to determine whether the message is from a valid source. Finally, SNMPv3 provides encryption, which is used to scramble the contents of a packet to prevent it from being seen by unauthorized sources.

A network has several devices and systems. They need to be monitored for their availability. Sometimes, it becomes difficult even to track these devices on the network. If a network device goes down or becomes unavailable, it is not easy to track them. The Simple Network Management Protocol, or SNMP, is the solution that meets all these requirements. SNMP helps you by:

- Identifying devices on a network – what type of device it is
- Tracking network changes – new devices are added, or older ones are removed
- Monitoring the network performance – health of the network
- Obtaining the device status – whether the device is functional or not

If SNMP is not used, then there is no way to perform the tasks mentioned above efficiently.

SNMP works with the client/server architecture where the managers and agents are the clients. The managers collate the information from the agents that are installed on the various network devices. It could be a server, a switch, or a router. The agents send the device information to the managers.

SNMP works in a hierarchical manner that contains:

- Management Information Bases (MIBs) for storing information in a hierarchical format. Each agent has a local MIB from which it sends the information to the managers.
- Object Identifiers (OIDs) are unique to each device being monitored. It is used to describe the state of the device.
- Traps to send information from the devices to the Managers



## *TOPIC 3*

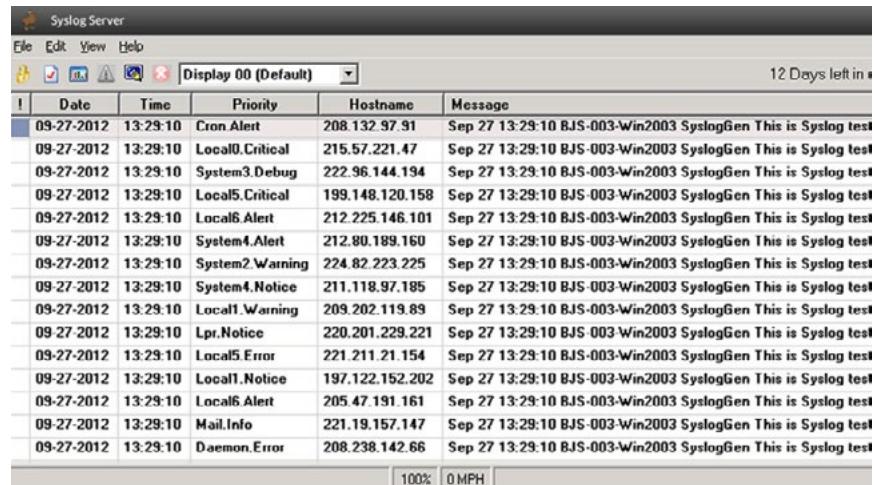
---

# NETWORK DEVICE LOGS

---

# Network Device Logs

- Is used to track the events that are taking place on a network and its devices
- Should be reviewed regularly to know the recent events that have taken place
- Use individual to each device but can be collated in a central server or device, such as syslog
- Types:
  - Traffic logs
  - Audit logs



The screenshot shows a software interface titled "Syslog Server". The main window displays a table of log entries with the following columns: Date, Time, Priority, Hostname, and Message. The table contains 15 rows of data, each representing a log entry. The "Message" column for all entries contains the text "SyslogGen This is Syslog test". The "Priority" column includes entries like "Cron.Alert", "Local0.Critical", "System3.Debug", etc. The "Hostname" column lists various IP addresses and hostnames. The "Date" and "Time" columns show the timestamp of each log entry.

Display 00 (Default)					
	Date	Time	Priority	Hostname	Message
09-27-2012	13:29:10	Cron.Alert	208.132.97.91	Sep 27 13:29:10 BJS-003-Win2003	SyslogGen This is Syslog test
09-27-2012	13:29:10	Local0.Critical	215.57.221.47	Sep 27 13:29:10 BJS-003-Win2003	SyslogGen This is Syslog test
09-27-2012	13:29:10	System3.Debug	222.96.144.194	Sep 27 13:29:10 BJS-003-Win2003	SyslogGen This is Syslog test
09-27-2012	13:29:10	Local5.Critical	199.148.120.158	Sep 27 13:29:10 BJS-003-Win2003	SyslogGen This is Syslog test
09-27-2012	13:29:10	Local6.Alert	212.225.146.101	Sep 27 13:29:10 BJS-003-Win2003	SyslogGen This is Syslog test
09-27-2012	13:29:10	System4.Alert	212.80.189.160	Sep 27 13:29:10 BJS-003-Win2003	SyslogGen This is Syslog test
09-27-2012	13:29:10	System2.Warning	224.82.223.225	Sep 27 13:29:10 BJS-003-Win2003	SyslogGen This is Syslog test
09-27-2012	13:29:10	System4.Notice	211.118.97.185	Sep 27 13:29:10 BJS-003-Win2003	SyslogGen This is Syslog test
09-27-2012	13:29:10	Local1.Warning	209.202.119.89	Sep 27 13:29:10 BJS-003-Win2003	SyslogGen This is Syslog test
09-27-2012	13:29:10	Lpr.Notice	220.201.229.221	Sep 27 13:29:10 BJS-003-Win2003	SyslogGen This is Syslog test
09-27-2012	13:29:10	Local5.Error	221.211.21.154	Sep 27 13:29:10 BJS-003-Win2003	SyslogGen This is Syslog test
09-27-2012	13:29:10	Local1.Notice	197.122.152.202	Sep 27 13:29:10 BJS-003-Win2003	SyslogGen This is Syslog test
09-27-2012	13:29:10	Local6.Alert	205.47.191.161	Sep 27 13:29:10 BJS-003-Win2003	SyslogGen This is Syslog test
09-27-2012	13:29:10	Mail.Info	221.19.157.147	Sep 27 13:29:10 BJS-003-Win2003	SyslogGen This is Syslog test
09-27-2012	13:29:10	Daemon.Error	208.238.142.66	Sep 27 13:29:10 BJS-003-Win2003	SyslogGen This is Syslog test

Network device logs are used for logging events on various network devices. Logs can provide a lot of information if you want to investigate an event. You can gather information, such as:

- Description of the event
- The time of the event
- Who triggered the event
- The device on which the event took place

Even though logs provide a lot of information, they need to be reviewed. Remember that the log review is a reactive action, not a proactive one. You need to regularly review the logs to ensure that the event can be handled as soon as possible.

While each device maintains its logs, they can still be configured to send them to a centralized server or device. You can configure the logs to be sent to a central server.

Then comes the traffic logs. A network would generate a lot of events, such as someone sending a message or someone browsing the Internet. Capturing every traffic event does not help, and you have to dig through a lot of "not-so-required" data. Therefore, selectively choose the type of traffic you need to capture in the form of events.

Audit logs are enabled for security purposes. For example, you may want to capture the event of password failure or failed login attempts. Enabling audit for every successful login may not help because if you have 1000 employees in the organization and everyone logs on in the first attempt, you have 1000 events logged that are not really of any use. On the other hand, if you log just the failed login attempts, you may have only a few selected failed login attempts. Therefore, carefully and selectively enable the audit logs.

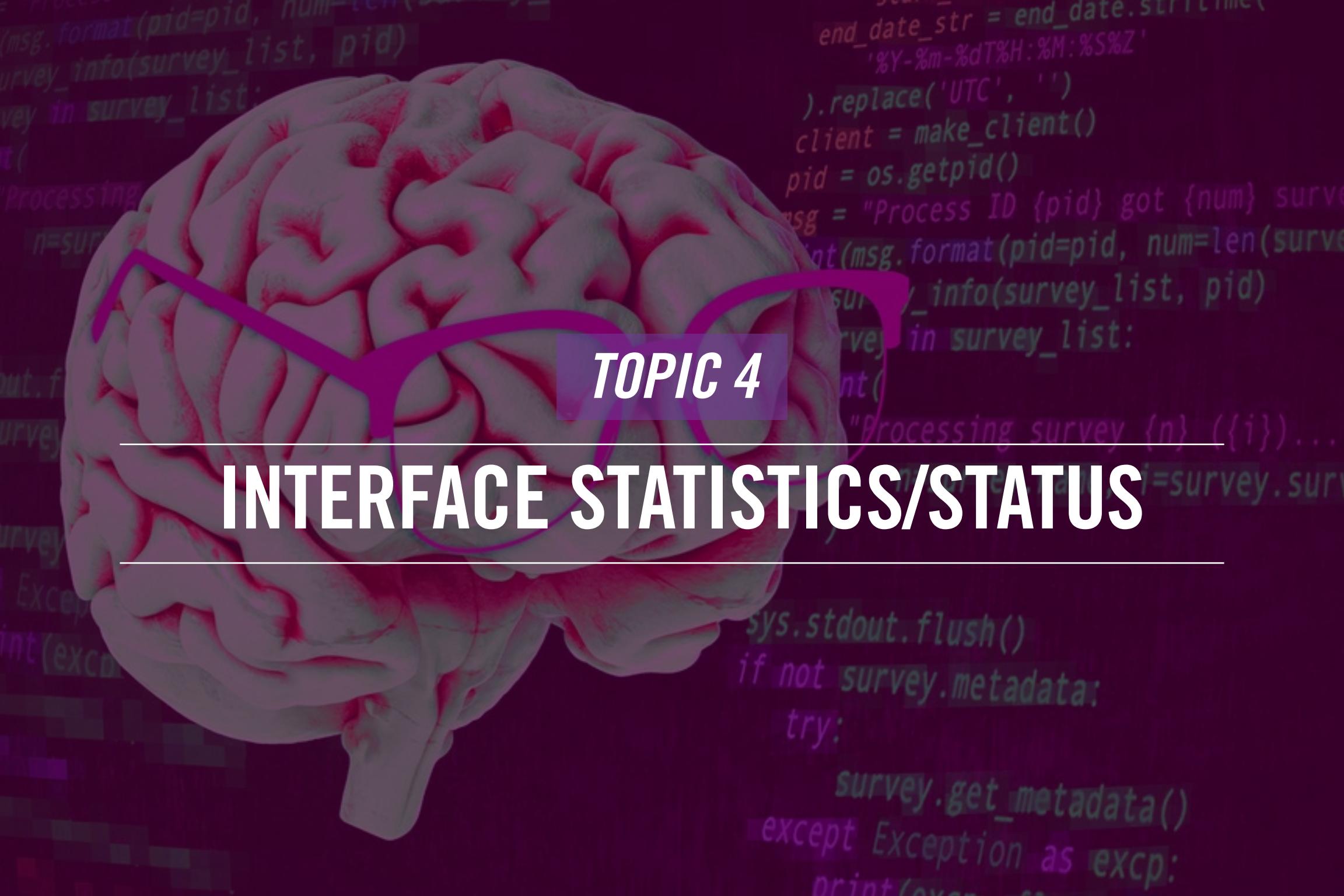
# Syslog Severity Levels

Level	Level Name	Syslog Definition	Description
0	Emergencies	LOG_EMERG	This level is used for the most severe error conditions, which render the system unusable.
1	Alerts	LOG_ALERT	This level is used to indicate conditions that need immediate attention from administrators.
2	Critical	LOG_CRIT	This level is used to indicate critical conditions, which are less than Alerts but still require administrator intervention.
3	Errors	LOG_ERR	This level is used to indicate errors within the system; however, these errors do not render the system unusable.
4	Warnings	LOG_WARNING	This level is used to indicate warning conditions about system operations that did not complete successfully.

Events can be identified with the severity, which has a particular designated number attached to them. These are widely accepted severity levels that most organizations adopt. However, some organizations may simply choose to use their severity levels.

The table shows that severity levels are divided into eight classes, ranging from 0 to 7. The lower the number, the more critical the event becomes. For example, an application cannot display a graphic – this can be a level 3, which is an Error.





## TOPIC 4

---

# INTERFACE STATISTICS/STATUS

---

# Interface Statistics/Status – Link Status

Protocol Packet  
and Byte Counts

Cyclic redundancy  
checks (CRCs)

Send/Receive Traffic

Speed/Duplex

Link State (Up/Down)

- Indicates the status of the network interface
  - Whether the link is up with a green color
  - Whether the link is down without any color
- Status can be indicated using the operating system tools, like Network and Sharing Center in Windows

When facing an issue with a network interface, the first thing you should check is the link status. Usually, most network interfaces have a light indicator that is on if the connection is live and working. If there is no light even after plugging in the Ethernet cable, there is an issue with the connection, which can either be the network interface or the cable or maybe the port on the switch. No color or light indicates some sort of an issue with the connection not being live.

Most of the operating systems like Windows and Linux have tools that help you determine the status of the network interface. You can check this in Network and Sharing Center in Windows. In the graphical mode of Linux, you have the network icon that displays its status.



# Interface Statistics/Status – Speed/Duplex

Protocol Packet and Byte Counts

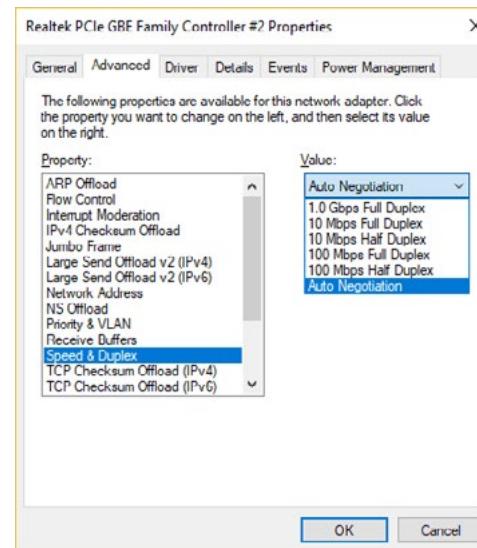
Cyclic redundancy checks (CRCs)

Send/Receive Traffic

Speed/Duplex

Link State (Up/Down)

- Is usually configured as Auto Negotiation as the default configuration
- Requires the both, the sender and receiver, to have the same speed and duplex



In recent years, network adapters or network interface cards have become smarter. They can configure the speed and duplex settings on their own. For example, in Windows, the speed and duplex settings are set to Auto-Negotiation, which allows the system to match the speed of the other device on the network for communication.

Two communicating devices need to match the speed and duplex settings. If they don't match, there is a communication failure that will take place.

# Interface Statistics/Status – Sent/Receive Traffic

Protocol Packet and Byte Counts

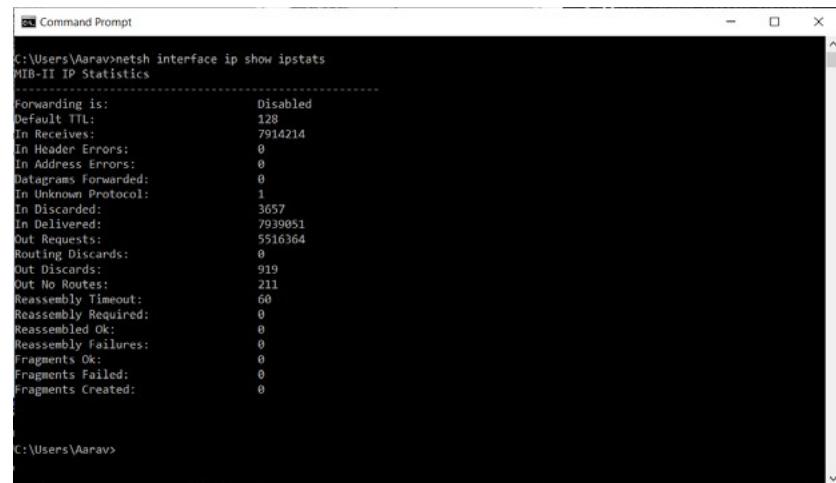
Cyclic redundancy checks (CRCs)

Send/Receive Traffic

Speed/Duplex

Link State (Up/Down)

- Is device sending and receiving packets as it should
- Can be checked on all devices, such as:
  - Router
  - Switches
  - Windows systems
  - Linux systems



The screenshot shows a Windows Command Prompt window titled "Command Prompt". The command entered is "netsh interface ip show ipstats". The output displays various statistics for the network interface, including:

Statistic	Value
Forwarding is:	Disabled
Default TTL:	128
In Receives:	7914214
In Header Errors:	0
In Address Errors:	0
Datagrams Forwarded:	0
In Unknown Protocol:	1
In Discarded:	3657
In Delivered:	7939851
Out Requests:	5516364
Routing Discards:	0
Out Discards:	919
Out No Routes:	211
Reassembly Timeout:	60
Reassembly Required:	0
Reassembled OK:	0
Reassembly Failures:	0
Fragments OK:	0
Fragments Failed:	0
Fragments Created:	0

C:\Users\Aarav>

Network interfaces in a device are meant to send and receive traffic. The network interface may also run into problems and fail to communicate with the other devices on the network. To ensure that the network interface is working, you should continuously monitor it. It should be able to send and receive traffic in the normal manner. For example, if you know that you are not sending out traffic, but you see a lot of outgoing packets, then it means something in the system is sending out the traffic. It could be malware that may be sending out information to its command-and-control center.

Almost all the network devices, such as a router, switches, and operating systems like Windows and Linux, provide this capability of monitoring the network interface.

# Interface Statistics/Status - CRCs

Protocol Packet  
and Byte Counts

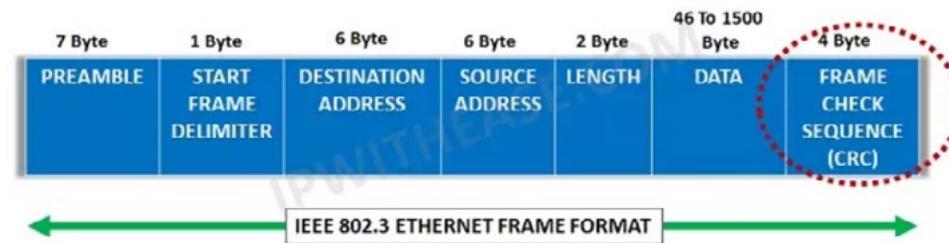
Cyclic redundancy  
checks (CRCs)

Send/Receive Traffic

Speed/Duplex

Link State (Up/Down)

- Performs error detection, not correction
- Is indicated by the 4-bytes in an Ethernet packet
- Indicates that packets are corrupt
- Performed at the sender and receiver end
  - Validates the data sent with the data received
- Can indicate a problem at the receiver end, during transmission
  - Can be due to the faulty cable
  - Can be due to collisions



[What is CRC \(Cyclic Redundancy Check\)? » Network Interview](#)

# Interface Statistics/Status - CRCs

The acronym CRC denotes Cyclic Redundancy Check, which is used to detect errors in network communication. It can be used to detect the mistakes of different data types that may be used on a system. For example, hard drives also use CRC, and if there are any errors, they alert the user of the error that occurs.

An Ethernet packet has an extra 4-byte long reserved for CRC., which is located next to the data section in the Ethernet packet.

When transmitting the data from one system to another system, a checksum, a precalculated value, is added to the data. The same checksum is also calculated and kept with the destination system. When the data arrives, the checksum is verified. If the checksum matches, this means that the data transmission is successful. However, there can be issues when you would have been notified that the data transmission to the destination failed. This is due to the destination system sending a negative acknowledgment to your system that the checksum of the data is not matching.

There can be various reasons for CRCs. It could be a problem at the receiving end, faulty cable, or even the network simply collisions that may be caused due to half-duplex communication.



# Interface Statistics/Status – Counts

Protocol Packet and Byte Counts

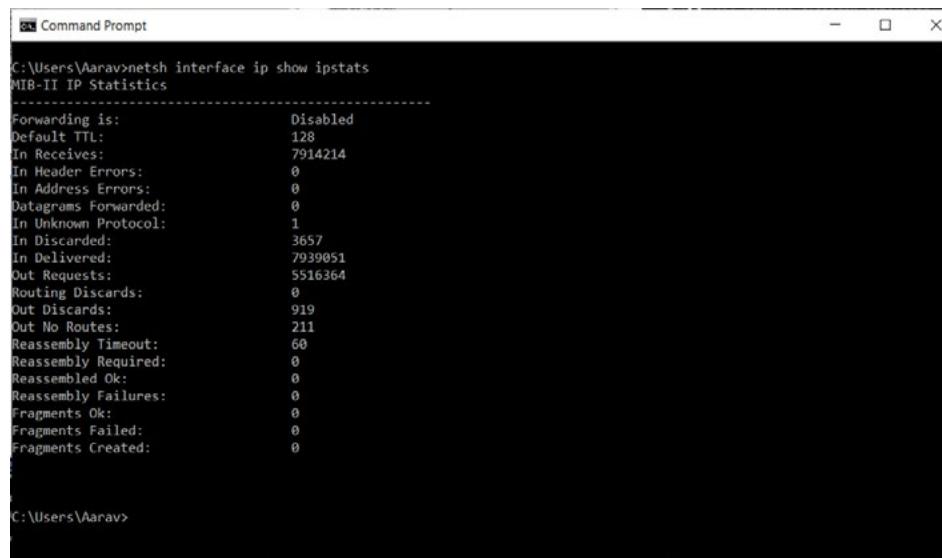
Cyclic redundancy checks (CRCs)

Send/Receive Traffic

Speed/Duplex

Link State (Up/Down)

- Indicates the number of packets coming in or going out through an interface
- Can be used for determining the status of the interface
- Can be used to determine if there is any malicious activity taking place



The screenshot shows a Windows Command Prompt window titled "Command Prompt". The command entered is "C:\Users\Aarav>netsh interface ip show ipstats". The output displays various statistics for an interface, including:

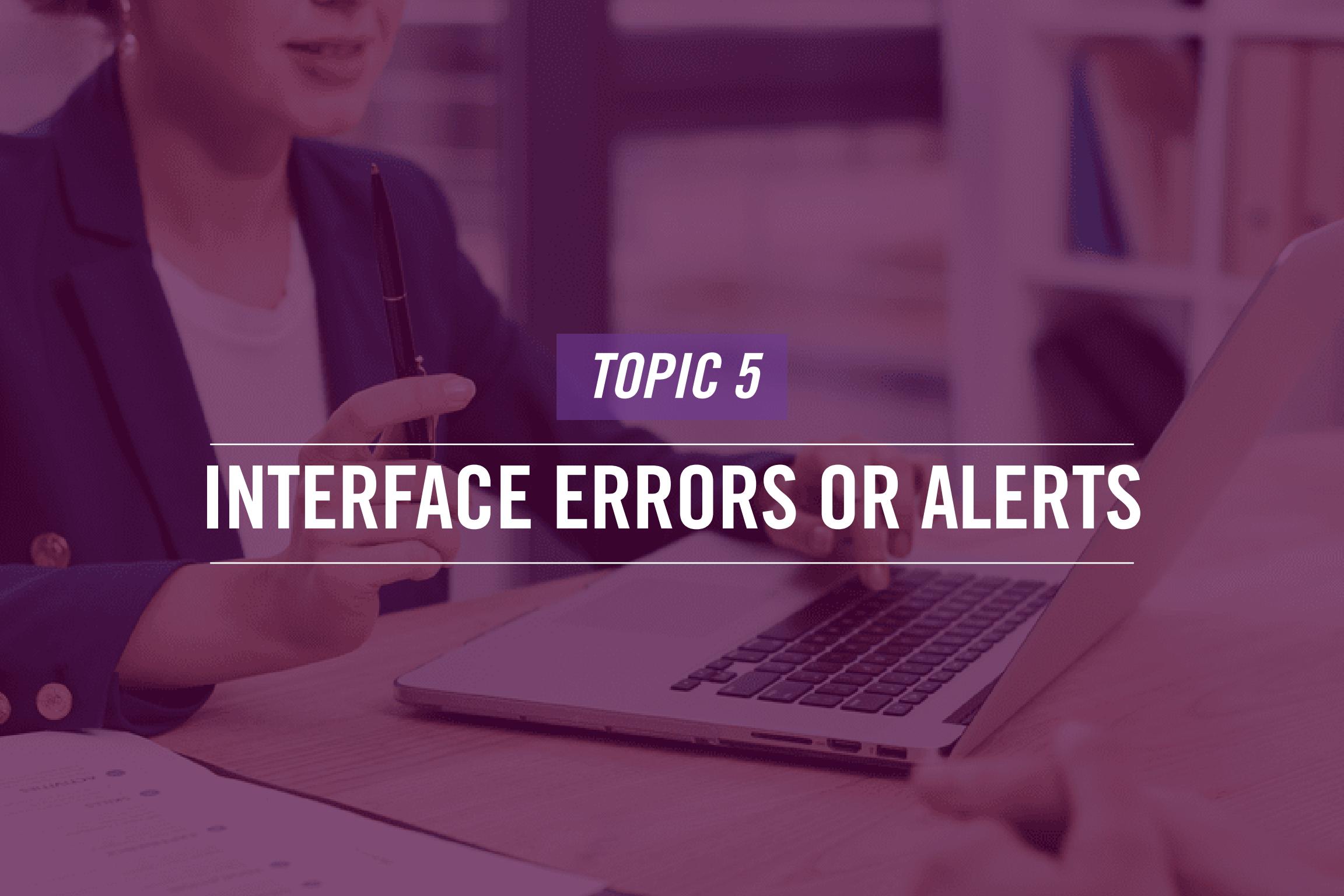
Statistic	Value
Forwarding is:	Disabled
Default TTL:	128
In Receives:	7914214
In Header Errors:	0
In Address Errors:	0
Datagrams Forwarded:	0
In Unknown Protocol:	1
In Discarded:	3657
In Delivered:	7939051
Out Requests:	5516364
Routing Discards:	0
Out Discards:	919
Out No Routes:	211
Reassembly Timeout:	60
Reassembly Required:	0
Reassembled Ok:	0
Reassembly Failures:	0
Fragments Ok:	0
Fragments Failed:	0
Fragments Created:	0

C:\Users\Aarav>

You may want to know the number of packets going out of a network interface. You may have a baseline that shows an average number of packets and a total number of bytes that the interface sends out in a specific period. If the number of packets has been multiplied to x times, you can suspect that something is happening in the system. It could be malware sending out information.

The information that you collate can provide the status of the network interface. If the number of packets is close to the data captured in the past, you know that the network interface is in a healthy state.

If there is an unusual number of packets going out of the system, you can suspect malicious activity. However, it is not good to conclude by just looking at the number of packets. Always inspect the system to understand the root cause.

A photograph of a person's hands working on a silver laptop keyboard. The person is wearing a dark long-sleeved shirt. A purple semi-transparent rectangular overlay covers the top half of the image. Inside this overlay, the words "TOPIC 5" are written in a white, bold, sans-serif font.

*TOPIC 5*

---

# INTERFACE ERRORS OR ALERTS

---

# Interface Errors or Alerts – CRC Errors

## Encapsulation Errors

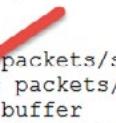
## Runts

## Giants

## CRC Errors

- Determines that the received packets are damaged or corrupted
- Can be due to speed or duplex mismatch
- Performed at the sender and receiver end
- Validates the data sent with the data received
- Can indicate a problem at the receiver end, during transmission
- Can be due to the faulty cable
- Can be due to collisions

```
Hardware is Lance, address is 0000.0c64.c401 (bia 0000.0c64.c401)
MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Full-duplex, 100Mb/s, media type is RJ45
ARP type: ARPA, ARP Timeout 04:00:00,
Last input 00:00:08, output 00:00:05, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0 (size/max/drops); Total output drops: 0
Queueing strategy: fifo
Output queue :0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
  0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
  0 input packets with dribble condition detected
  0 packets output, 0 bytes, 0 underruns
  0 output errors, 0 collisions, 1 interface resets
  0 babbles, 0 late collision, 0 deferred
  0 lost carrier, 0 no carrier
--More-- |
```



When a system receives a packet, its checksum is checked to ensure that it is intact and is not corrupt.

As stated earlier, the checksum is calculated at the sender and receiver's end. If there is a difference in the checksum after the packet is received, the packet is corrupt or has some issue. This triggers a CRC error message to the user.

The key reasons for the CRC error can be a faulty cable, or even the network simply collisions that may be caused due to half-duplex communication.



# Interface Errors or Alerts – CRC Errors

Encapsulation Errors

Runts

Giants

CRC Errors

- Is an Ethernet packet that is larger than 1518 bytes in size
- Can be due to:
  - Environment configuration
  - Hardware problem, such as a bad network adapter
  - Driver problem
  - Incorrect duplex or speed settings

An Ethernet packet has the default size of 1518 bytes. A giant packet is larger than the default size. This can be due to the changes in the network configuration. For example, the network is configured to use giant packets, but this becomes a little unusual. Therefore, in most cases, the giant packets are due to technical issues, such as:

- Hardware problem – network interface card is malfunctioning
- Driver problem – the network interface card's driver is incompatible or corrupt
- Incorrect duplex or speed – the duplex, half-or full-duplex, and speed mismatch



# Interface Errors or Alerts – Runts

Encapsulation Errors

Runts

Giants

CRC Errors

- Are packets that are smaller than the normal size – typically less than 64 bytes
- Can be due to:
  - Hardware problem
  - Driver issue
  - Network collisions

```
GigabitEthernet1/0/13 is up, line protocol is up (connected)
Hardware is Gigabit Ethernet, address is 4cbc.4843.300d (bia 4cbc.4843.300d)
Description: MAIN-P2P
MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
reliability 255/255, txload 2/255, rxload 3/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Full-duplex, 1000Mb/s, media type is 10/100/1000BaseTX
input flow-control is on, output flow-control is unsupported
ARP type: ARP, ARP Timeout 04:00:00
Last input never, output 00:00:00, output hang never
Last clearing of "show interface" counters never
Input queue: 0/2000/0/0 (size/max/drops/flushes); Total output drops: 1141242
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 12204000 bits/sec, 1900 packets/sec
5 minute output rate 9630000 bits/sec, 1719 packets/sec
1753779818 packets input, 1736052869482 bytes, 0 no buffer
Received 11016866 broadcasts (6989959 multicasts)
13 runts, 94464 giants, 0 throttles
718600 input errors, 54 CRC, 0 frame, 0 overrun, 0 ignored
0 watchdog, 6989959 multicast, 0 pause input
0 input packets with dribble condition detected
1432492803 packets output, 951276894099 bytes, 0 underruns
0 output errors, 0 collisions, 2 interface resets
0 unknown protocol drops
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier, 0 pause output
0 output buffer failures, 0 output buffers swapped out
no arp source guard
```

Where giants are large packets, the runts are packets that have less than 64 bytes size. They also occur due to the faulty network interface card or sometimes due to incompatible or corrupt drivers. Network collisions can also cause runts. It is pretty common for collisions to occur in a half-duplex communication. In such collisions, the runts are dropped due to smaller packet sizes.



# Interface Errors or Alerts – Encapsulation Error

## Encapsulation Errors

### Runts

### Giants

### CRC Errors

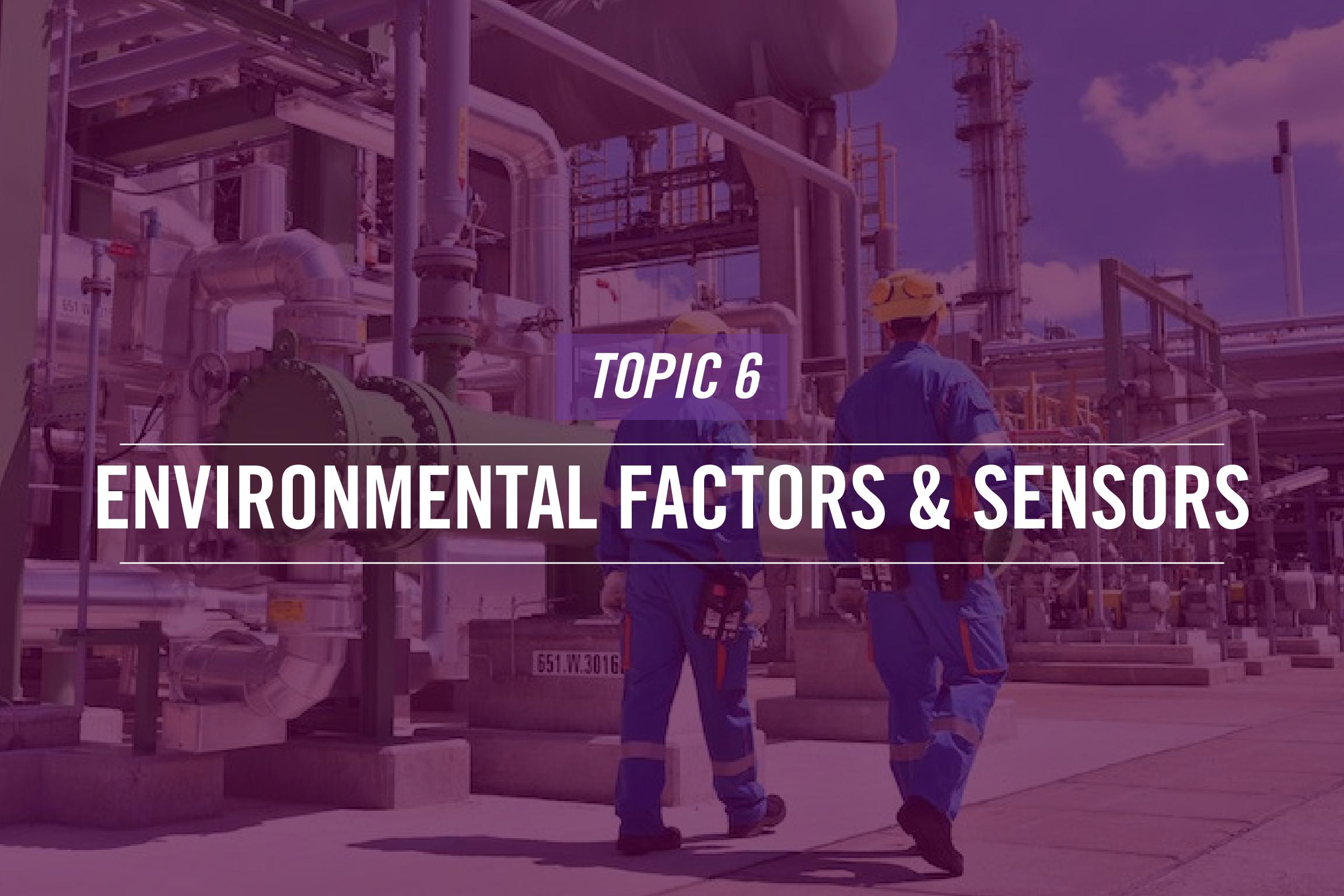
- Are due to Incorrect encapsulation method used by a network adapter
- Take place as some part of the Layer 2 header has missing elements
- Need to be monitored closely to be tracked

In the networking world, encapsulation is the method of adding extra bytes to the headers and trailers of the packets. With encapsulation, the packets are wrapped with more information. However, if the network does not support the encapsulated packets, then the encapsulation error occurs. It can be caused due to the incorrect encapsulation of a network interface card.

When a packet is at Layer 3 and needs to be forwarded, it needs to carry the information from Layer 2. However, if some pieces of the information are missing from Layer 2, it results in the encapsulation error message.

When encapsulation errors are encountered, they need to be monitored closely. If the problem is due to the incorrect encapsulation method on the network interface card, it can be corrected with minimum effort.





*TOPIC 6*

---

# ENVIRONMENTAL FACTORS & SENSORS

---

# Environmental Factors and Sensors

- Temperature
  - Can crash the systems if weather is too hot inside the datacenter
  - Requires around 80 degrees of temperature in the datacenters
- Humidity
  - Can cause condensation build-up causing corrosion in devices
  - Can also cause short-circuits
- Electrical
  - Can cause fire due to unshielded and uncovered power cables
  - Need to have redundancy
- Flooding
  - Can cause damage to the entire datacenter, which should be located on the upper floors or raised floors



# Environmental Factors and Sensors

Several environmental factors play a crucial role in the smooth functioning of a datacenter. Some of the key ones are temperature, humidity, electrical, and flooding. Let's now look at each one of them.

Too much heat within a datacenter can cause various issues. For example, the servers and devices can crash or continue to reboot due to heat. When you talk about the temperature, it needs to be just optimum, around 80 degrees. The placement of racks within a datacenter plays a key role in keeping the temperature at an optimum level. For example, the backs of the racks should be facing each other. Racks draw cold air from the front, and if you put the back of a rack in front of another one, then hot air will go out of the back and will be absorbed from the front, which would not help.

Humidity in a datacenter is another challenge. The heat within the datacenter decreases humidity. However, too much heat, as stated earlier, causes other issues like reboots. You need to keep the heat and humidity at an optimum level. For humidity, you need to have moisture in the air. However, too much moisture can also cause various issues like corrosion in network devices. It can also cause short-circuits. High humidity causes corrosion. On the other hand, low humidity causes static electricity that can damage the network devices and other equipment.

There can be electrical issues. If some unshielded wires or wires have cuts, they can cause a fire. Therefore, each cable must be properly covered. If there are damaged wires, you should replace them immediately. On the other hand, you should also have redundancy for electricity. You should be able to source it from more than one source.

Your datacenter might be in an area that is prone to flooding, which can destroy the datacenter. Usually, several organizations build the datacenter on the ground floor, which is quite a risk if it is a flood-prone area. To avoid this, you should either build the datacenter on the upper floors or on the raised floors where water should not reach.

All these environmental factors can be handled with the use of sensors.





# **TOPIC 7**

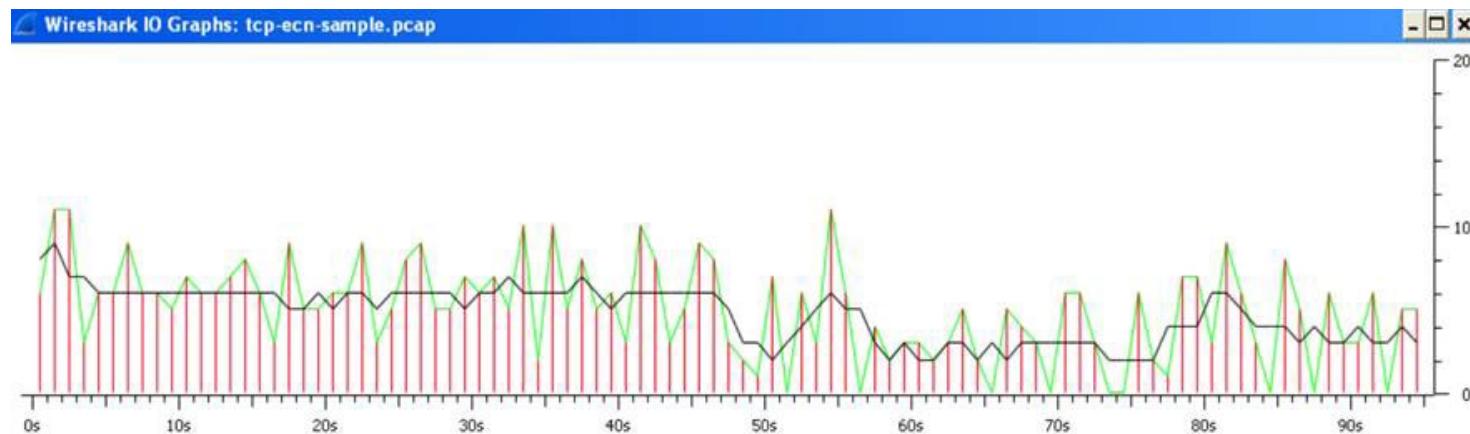
---

# **BASELINES**

---

# Baselines

- Defines the normal utilization of a system or network
- Is created based on the data from the past
- Is used for discovering the deviation from the current metrics
- Is used for troubleshooting the system or network devices
- Can also be used for making changes in the system or network

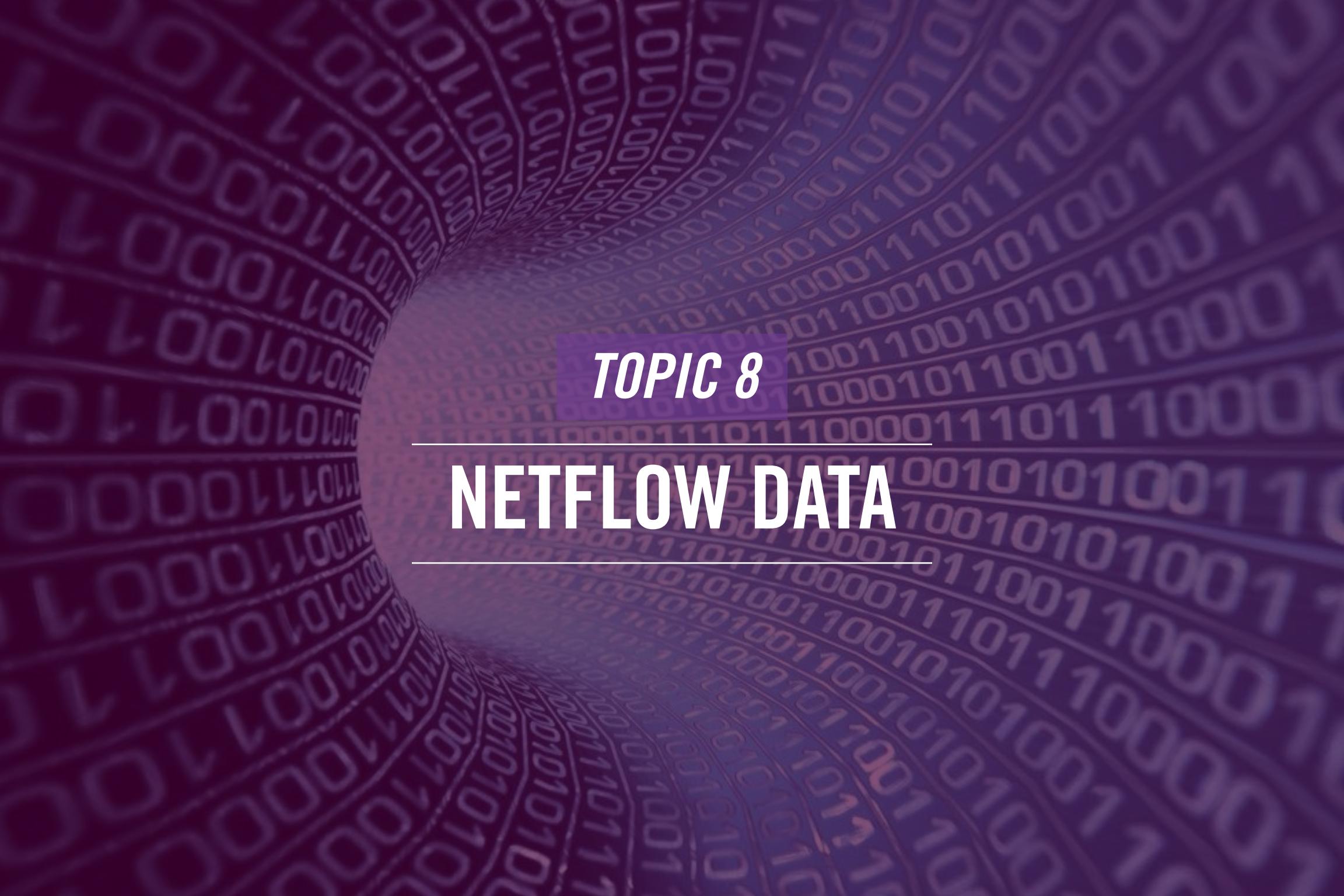


Every organization expects the network to work in a normal manner or way. The normal way or manner is defined through a baseline. It defines the normal utilization of the network or a system. For example, the network traffic should always be half of its total capacity – that's the normal way or utilization. You can define the total capacity and its half, which becomes the baseline. If the network utilization goes above the halfway mark, you have to investigate how it happened.

You create a baseline from the data you gathered in the past. A baseline should not be created with assumptions. The past data can come from logs or network monitoring. Once you have defined the threshold for the normal level, you can create a baseline.

After creating the baseline, you can determine if the network or a system is performing optimally. You can also use it to determine several issues like network congestion or even high CPU utilization in a system.

With the baseline, you not only detect the deviations, but if the deviations are consistent, you may have to make changes to the baseline itself. For example, you created a baseline without an internal application that was launched later. With the launch of the application, there was a certain level of traffic generated, which added to the baseline threshold. There is an obvious deviation because this is add-on traffic. This will require the baseline to change to accommodate the new traffic.



**TOPIC 8**

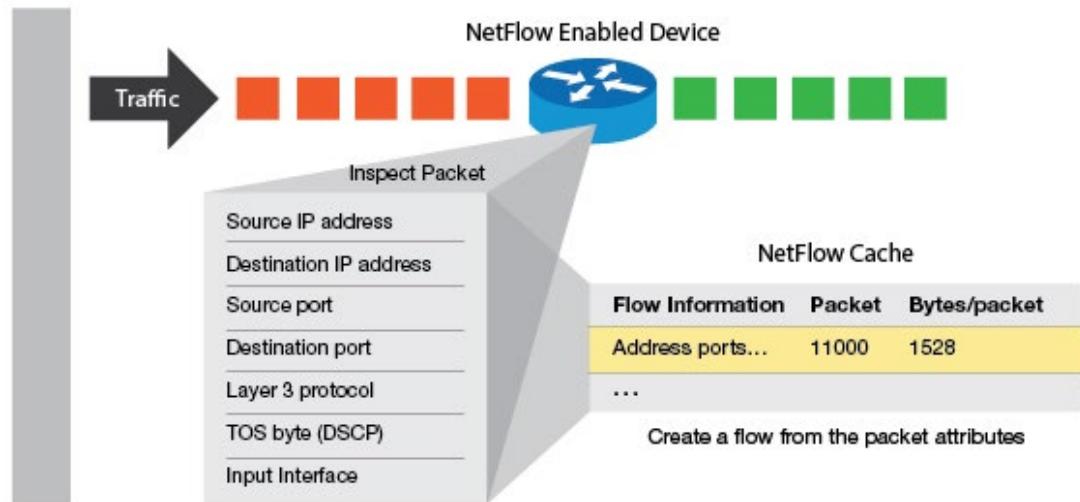
---

**NETFLOW DATA**

---

# NetFlow

- Is a proprietary Cisco protocol for network traffic monitoring
- Helps the network administrator in:
  - Monitoring the network
  - Planning the future extension
  - Performing analysis of the captured data
- Uses visualizations to display the captured traffic and users' access to the network services
  - Helps to determine the network utilization
  - Helps to detect user behavior anomalies



Netflow is a proprietary Cisco protocol for network monitoring. It can gather a lot of information about the traffic that is flowing on the network. One of the reasons you monitor the network traffic is to perform analysis and find certain patterns in the traffic. This can help you narrow down several types of network issues. For example, if there is network congestion, you can monitor traffic to find the origin from where it is happening.

You can use NetFlow in different ways. You can use it for:

- Network Monitoring: To visualize and build the traffic patterns
- Network Planning: To plan for future growth, such as adding more switches and routers to cater to the high network traffic flow or even increasing the bandwidth to avoid congestion.
- Traffic Analysis: To monitor the network traffic and build patterns that can be used to detect deviations. This can help in traffic a change in the traffic pattern, if any. For example, if malware starts to cause network congestion, it can be detected as the traffic pattern would differ, and there would be an increase in traffic volume.

NetFlow helps the network administrator build visualizations of the traffic patterns to determine the way network and its services are being used. With the captured data, a baseline can be determined. The network administrator can also use the baseline to determine the anomalies by detecting the change in the network traffic.

***TOPIC 9***

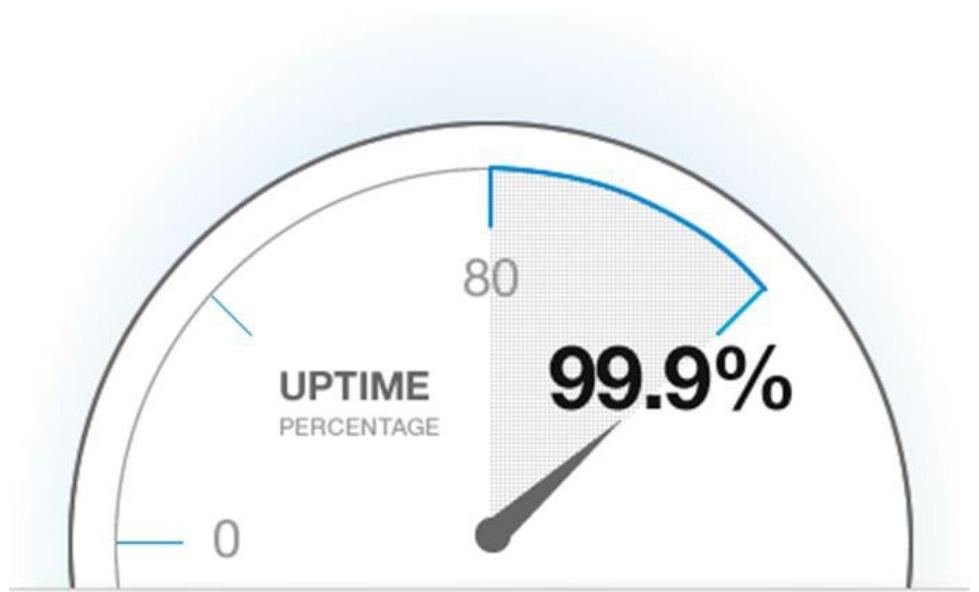
---

# UPTIME/DOWNTIME

---

# Uptime/Downtime

- **Uptime**
  - Is the amount of time a service or device has been running
  - Is expected to be 99.999%
  - Is committed by the service provider
- **Downtime**
  - Is the amount of time when a system or service is unavailable to provide services
  - Can be planned (network maintenance, configuration updates) or unplanned (natural disaster, incorrect configurations)



# Uptime/Downtime

Uptime is also known as availability. It is the time that a network, system, or service is up and running. For example, if a webserver has been running for last 364 days in a year, you can calculate the uptime with the following formula:

$$\frac{\text{Total number of hours a server/service is up and running}}{\text{Total number of hours in a year (24 x 365 days = 8760)}} \times 100$$

When you use this formula:

$364/365 \times 100$   
You get the uptime as 99.988.

A service provider, such as a cloud service provider, would promise a certain uptime, 99.999 percent.

One would expect the uptime to be 100%, but it is impossible to achieve in the technology world. It is a wish that you can achieve 100% uptime. Rather, most organizations focus on the 99.999% uptime, which is still difficult to achieve but not impossible. It is not realistic to imagine a 100 percent uptime because you would be performing certain maintenance on a server due to which you need to bring it down. Taking a server or service offline is downtime.

If the uptime is the amount of time a service or system is up and running, the downtime is just the opposite of it. It is the amount of time a service or system is unavailable or nonfunctional. For example, an internal HR system is inaccessible through a Web browser. This is the downtime. You can have a planned or unplanned downtime. Planned downtime is scheduled and planned properly. For example, if you visit your organization's HR system, it flashes a notification that there is a planned downtime coming Sunday from 1:00 AM to 5:00 AM. On the other hand, unplanned downtime is when the service or system goes down unexpectedly. It could be due to various reasons like a flood, a natural disaster, or human error, or even incorrect configuration changes, something like incorrectly modifying the Web server's configuration file.



# Summary

- Performance Metrics/Sensors
- SNMP
- Network Device Logs
- Interface Statistics/Status
- Interface Errors or Alerts
- Environmental Factors and Sensors
- Baselines
- NetFlow Data
- Uptime/Downtime



That's the end of the lesson.

Here we covered:

- Performance Metrics/Sensors
- SNMP
- Network Device Logs
- Interface Statistics/Status
- Interface Errors or Alerts
- Environmental Factors and Sensors
- Baselines
- NetFlow Data
- Uptime/Downtime

*NEXT TOPIC*

---

# ORGANIZATIONAL DOCUMENTS AND POLICIES

---

Lesson

# 2

# Organizational Documents and Policies

- 1 — Welcome to the lesson 2 of Module 3. In this lesson, you will learn about the:
- 2 — Organizational Documents and Policies



Network Fundamentals

# Agenda

- Plans and procedures
- Hardening and Security Policies
- Common Documentation
- Common Agreements

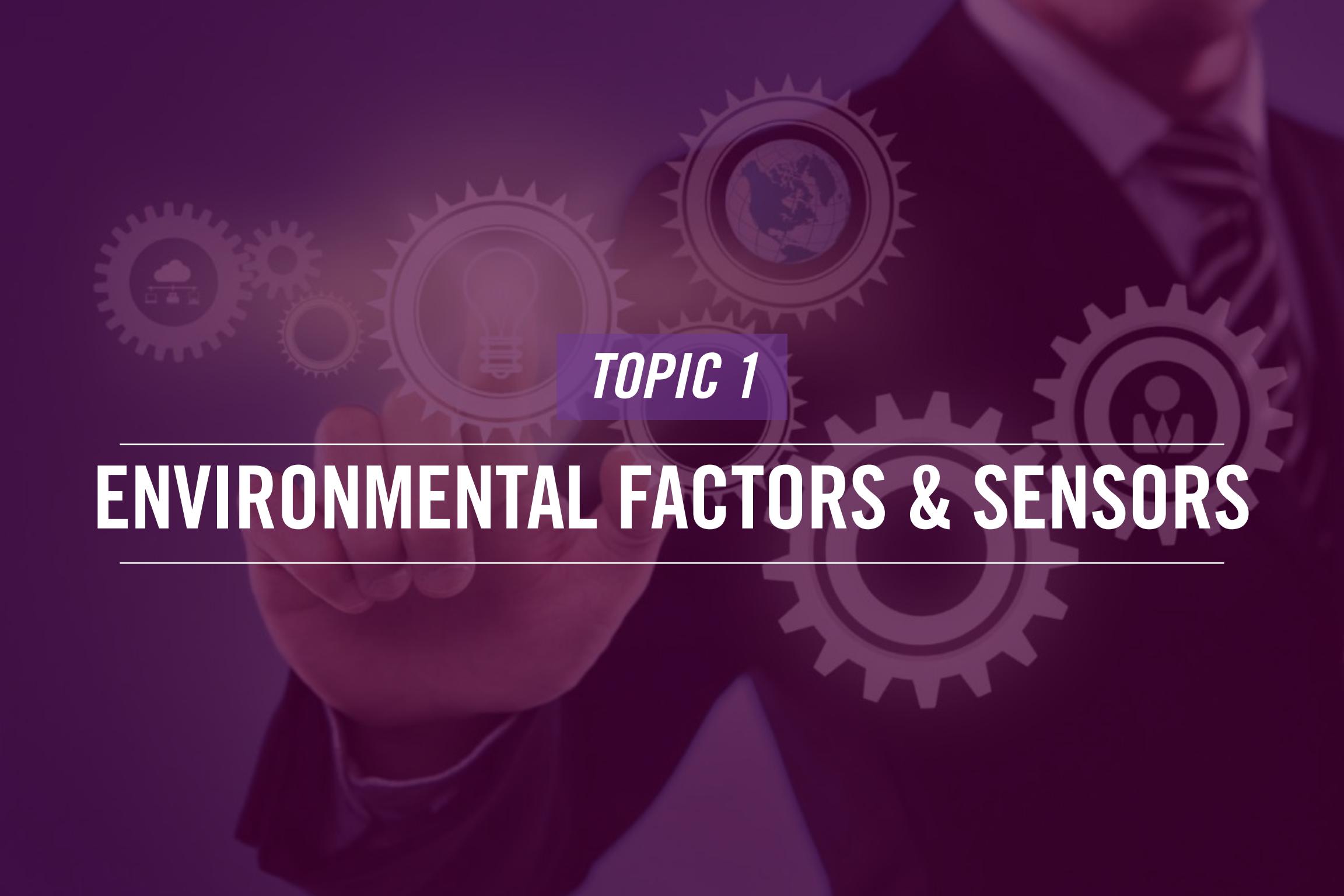


Hi, welcome to COMPTIA Network+ Course

In this lesson, we will talk about:

- Plans and procedures
- Hardening and Security Policies
- Common Documentation
- Common Agreements





## *TOPIC 1*

---

# ENVIRONMENTAL FACTORS & SENSORS

---

# Change Management

Standard Operating Procedures

System Life Cycle

Business Continuity Plan

Disaster Recovery Plan

Incident Response Plan

Change Management

- Helps an organization track changes in the infrastructure
- Implements the Change Management Policy that defines:
  - Identification of changes
  - Backups before implementing changes
  - Rollback plans in case of change fails
  - Plan for change management – time, approvals, resources
- Defines the change approving authorities
- Helps to document changes that have been implemented



# Change Management

Changes in any environment are inevitable. They are likely to happen. The IT environment is highly dynamic, and changes take place at a rapid pace. For example, a new security control implementation is a change. However, changes may not always bring the results that you want them to. To ensure that changes do not introduce unwanted and undesirable results in the IT environment, you should implement change management. Even a minor modification in the network can have a highly negative impact, such as making a few network services unavailable. However, it could have been protected if a change management plan mentioned the change management process that controls the changes to be implemented.

When anyone in the IT team wants to implement a change, it has to be approved. The change management policy defines the complete process for change management. The policy also defines the steps that must be performed during the change management process. For example, you need first to identify the change that needs to be implemented. You also need to include the rollback plan available if the change does not produce desirable results. There will be situations where backups need to be performed. For example, let's say that you need to upgrade a Windows Server to the latest version. You would need to perform a backup. Along with this, did you test how the upgrade works in a similar test environment?

Before you proceed to get the approval for the change to be implemented, you need to test the change and record the output, including the date and time for the test. Then, you build a case to showcase it to the change approving authorities. After their formal go ahead, you can implement the changes and document the results.

The steps that have been broadly defined must be included as part of the change management policy.



# Incident Response Plan

Standard Operating Procedures

System Life Cycle

Business Continuity Plan

Disaster Recovery Plan

Incident Response Plan

Change Management

- Helps an organization to respond to an incident
- Defines the steps to be performed when an incident takes place
- Needs to be created before hand, not after an incident
- Defines key components like:
  - Scope
  - Definition
  - Procedures
  - Roles and responsibilities



# Incident Response Plan

Just like the changes, incidents are also bound to happen. A change may produce an unwanted result, which eventually turns into an incident. The organization needs to have an incident response plan to handle the incidents that may occur.

Incidents can be of any nature, right from a server crash to a denial-of-service (DoS) attack on a webserver. Therefore, the incident response plan is not specific to a kind of incident, but it is generic in that it provides the instructions to handle all types of incidents. For example, it has several phases: Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned.

It is important that the organization creates the plan and keeps it ready for emergencies. It should be created, tested, and finalized for any incident to be handled. You should not wait for an incident to occur to create this plan because this plan helps you with the right decisions during an incident.

First, you need to create the incident management policy that defines the need for creating the Incident Response Plan, which contains a few critical components like:

- The need and scope of the incident response plan
- Definitions of the different levels of incidents
- Procedures for handling different types of incidents
- Roles and Responsibilities of the incident response team



# Disaster Recovery Plan

Standard Operating Procedures

System Life Cycle

Business Continuity Plan

Disaster Recovery Plan

Incident Response Plan

Change Management

- Is a reactive approach to handling a disaster
- Is a capability that an organization has
- Helps to minimize the impact of a disaster and helps in speedy recovery
- Helps to minimize the data loss
- Focuses on the restoration of IT operations
- Is part of the business continuity plan



# Incident Response Plan

A disaster recovery plan is a reactive approach to handle a disaster. The organization needs to build the disaster management capabilities that are guided through the disaster recovery plan. Assume that you don't have this plan and a major disaster has taken place. One of your sites has become non-operational due to the disaster. What would you do in that case? Well, if you do not have the disaster recovery plan, then it is obvious that you will be running from pillar to post to handle that disaster. On the other hand, let's assume that you have a disaster recovery plan. You would know exactly what to do if a certain type of disaster occurs.

The key purpose of the disaster recovery plan is to:

- Be ready for the unplanned disasters
- Minimize the impact of the disaster as much as possible
- Recover the business operations with speed and agility and minimize the data loss to a great extent

There are various tasks that you need to perform as per the disaster recovery plan. You need to plan for the alternate locations, data backup and restoration methods, set up a team who would act during the disaster, define their roles and responsibilities, and first and foremost, identify the overall scope of the disaster recovery plan. The overall intent of the disaster recovery plan should be the speedy recovery of the IT operations.

It is important to note that a disaster recovery plan is not created in isolation. It is part of an organisation's strategic decisions that drive it to put business continuity in place. Therefore, you can say that disaster recovery is part of the big picture, the business continuity, which is discussed next.



# Business Continuity Plan

Standard Operating Procedures

System Life Cycle

**Business Continuity Plan**

Disaster Recovery Plan

Incident Response Plan

Change Management

- Is a strategy defined by an organization to ensure continuity of operations before, during, and after the disasters
- Minimizes the downtime
- Is invoked when a disaster strikes
- Requires:
  - Identification of services with their priorities
  - Risk assessment to be performed
  - Creation of recovery procedures
  - Communication with the users and stakeholders
  - Testing the plan and updating accordingly
  - Training the users
  - Maintaining the plan with continuous updates if required



# Business Continuity Plan

Before understanding a business continuity plan, it is essential to understand what business continuity is. Business continuity is the beforehand preparation of a disaster. This means that the organization has put in efforts to implement measures and controls to help an organization survive when a disaster strikes. The organization with business continuity is ready to handle the disaster in a planned manner and continue its business operations with minimal or no impact. The intent is to survive the disaster without disrupting the business operations.

For example, when a disaster strikes, the organization should continue to communicate with the customers, relocate its employee to another location, or even keep its IT operations functioning.

Let's now talk about the business continuity plan, a proactive approach to handling a disaster. The organization wants to ensure the continuity of its operations during and after the disaster similarly as it was before the disaster. You want to minimize the disruption to the IT operations during a disaster, which is what the business continuity plan is meant for. You need to be ready beforehand. The disaster may leave a short-term or long-term impact. The business continuity plan should define the strategy to handle these impacts. You invoke the business continuity plan only when a disaster strikes, but you need to keep it ready. You need to test it out and ensure that it works. There should not be any last-minute surprises.

You need to have a business continuity team that creates, tests, and implements a business continuity plan, which should be created with the following steps:

- You need to identify the business operations and services and prioritize them. This will help you decide what will be moved first and last.
- You need to conduct business impact analysis – what will be the impact of a disaster?
- You need to perform a risk assessment
- You need to create recovery procedures that will be used during and post-disaster phase
- You need to test the plan and ensure that it integrates with the rest of the services. For example, adding high availability to the servers and applications can be part of a business continuity strategy.
- Test the plan thoroughly and make changes if required. After testing the plan, you need to start implementing it. You may have to procure software and hardware.
- After its rollout, you need to now document and then train the users.
- Finally, you need to maintain it.

# System Life Cycle

Standard Operating Procedures

System Life Cycle

Business Continuity Plan

Disaster Recovery Plan

Incident Response Plan

Change Management

- Is the time that a device spends in an organization:
  - Acquisition
  - Implementation
  - Maintenance
  - Decommissioning
- Requires careful decommissioning at the end to prevent any data leakage



# System Life Cycle

When an organization buys a piece of hardware, it has a usability period beyond which it is not used. The total time from purchase to decommissioning of the device is the system life cycle, consisting of four different phases.

- Acquisition: It is the first phase of the system life cycle. In this phase, it is a procedure labeled as an asset and identified with a specific number or label. Each organization has a different method of asset identification, so accordingly, the device is labeled.
- Implementation: After the acquisition phase is over, the device is implemented. Depending on the type of asset, it is used accordingly. If it is a wireless access point, it is installed and configured.
- Maintenance: This phase may or may not occur in every device's lifetime. The maintenance phase is used when the device breaks down or needs some service. For example, if a server rack continues to function without any issue, it does not require going into the maintenance phase.
- Decommissioning: At the end of the system life cycle comes to the decommissioning phase. For example, several organizations have the policy to decommission the laptops after three years. However, depending on the device the organization is decommissioning, it must ensure no data or configuration is stored on them. This is a critical phase and needs a careful data removal strategy to prevent data leaks with the devices.



# Standard Operating Procedures

## Standard Operating Procedures

System Life Cycle

- Are set of instructions to perform a task
- Bring operational consistency as everyone follows the same steps
- Reduces the chances of human error
- Focuses on what needs to be done, not on how it needs to be done
- Has components, such as:
  - Purpose
  - Scope
  - Responsibilities
  - Definitions
  - Procedures

Business Continuity Plan

Disaster Recovery Plan

Incident Response Plan

Change Management



# Standard Operating Procedures

Every organization performs several operations, which are carried out systematically. Some instructions tell you what needs to be done in these operations. These instructions are known as the standard operating procedure. Let's take an example of a backup process that states how the backup needs to be performed. It is not defining the step-by-step instructions rather defining that it should be a combination of differential and full backup as an example.

When you implement standard operating procedures, they should be followed by everyone. There are usually several standard operating procedures for IT operations that need to be followed by them. Since everyone receives the same set of instructions using the standard operating procedures, there are fewer chances of error. Because every time the same steps are followed, there are fewer errors, which eventually increases productivity. The organization saves time and cost.

The following components need to be included in the standard operating procedures:

- Purpose
- Scope
- Responsibilities
- Definitions
- Procedures





## *TOPIC 2*

---

# HARDENING AND SECURITY POLICIES

---

# Password Policy

Data Loss  
Prevention Policy

Security Policy

Onboarding and  
Offboarding Policy

Remote Access Policy

Bring Your Own  
Device (BYOD) Policy

Acceptable Use Policy

Password Policy

- Defines the password requirements for an organization
- Is implemented using Group Policy in Windows environment
- Contains instructions to define a password
- Defines:
  - Password history
  - Minimum and maximum password age
  - Minimum password length
  - Password complexity
- Is shared and made available to the users



# Password Policy

In an organization, a password policy defines how the password should be formed. Most users have the habit of using easy passwords, such as a password. The password ‘password’ is still one of the most used passwords on the Internet. It is easy to guess, and password cracking tools will take less than a second to crack this password.

When it comes to passwords, the users within the organizations should not choose a simple password. The password policy should define the need and mandate to use complex passwords, which can then be enforced through Group Policies in the Windows environment. For example, the password policy should define the minimum number of characters in the password, whether it should be complex, and how many days the user must change the password.

In Group Policies, you can configure several parameters for the password policy. You can enable:

**Password history:** The number of passwords a user cannot re-use. For example, if you set this to 3, the user cannot re-use the last three passwords. However, as the user changes the password next time, the first password becomes available for re-use.

**Minimum and maximum password age:** When a user sets the password, there is a minimum age. For example, let's say it is one day. If the user changes the password today, then in the next 24 hours, the user cannot change the password. After the duration of 24 hours is over, the user can change the password. Similarly, the maximum password age defines the number of days a user can use the same password.

**Minimum Password Length:** It defines the minimum number of characters a password should have.

**Passwords complexity:** The combination of = letters, numbers, and special characters must be used to form a password. In Group Policies, the username cannot be included in the password.

Even though an organization, if using Windows domain, can implement the password policy using Group policy, it should be a written document. The users should be informed of this document.

# Acceptable Use Policy

Data Loss  
Prevention Policy

Security Policy

Onboarding and  
Offboarding Policy

Remote Access Policy

Bring Your Own  
Device (BYOD) Policy

Acceptable  
Use Policy

Password Policy

- Is also known as Acceptable Usage Policy or AUP
- Defines how the network, its devices, and services should be used by the users
- Highlights the consequences for violation of the policy
- Contains key components, such as:
  - Dos and Don'ts – what actions can or cannot be performed
  - Unacceptable usage definition and actions that should not be performed
  - Exceptions
  - Non-compliance consequences



# Acceptable Use Policy

Organizations always have dos and don'ts about organizational behavior, project execution, and many other things. When it comes to the IT infrastructure, organizations usually have an Acceptable Use Policy (AUP) policy. AUP intends to enforce the correct usage of network devices and resources. For example, the users should not be playing online games. The Internet is to be used only for official purposes.

Several organizations now attempt to get the AUP signed when a new user joins. The user is asked to read the AUP document and then sign it. This is done to ensure that the user later cannot deny the correct usage of the resources.

The AUP document highlights the consequences that users may have to bear if they do not abide by the dos and don'ts mentioned in the AUP. For example, there is a clear mention of the improper usage:

- Playing online games
- Visiting adult websites
- Using an organization's resources for personal or illegal use like hacking

Some of the components of the AUP are:

- Concerned users – to whom does this policy apply
- Reason for AUP – defines the objective and scope of AUP
- Acceptable use guidelines – what is considered as acceptable usage and what users should be doing
- Unacceptable use – what is considered as an unacceptable usage
- Exceptions – what is not included in the scope of AUP
- Non-compliance or sanctions – what actions need to be taken if there is a violation of AUP



# Bring Your Own Device (BYOD) Policy

Data Loss  
Prevention Policy

Security Policy

Onboarding and  
Offboarding Policy

Remote Access Policy

Bring Your Own  
Device (BYOD) Policy

Acceptable  
Use Policy

Password Policy

- Is defined by an organization to allow the users to bring their personal devices for official work
- Defines the types of devices can be used
  - Models
  - Ownership of the information on personal devices
  - Types of apps used
- Can enforce the use of Mobile Device Management (MDM) to protect information in BYOD devices



# Bring Your Own Device (BYOD) Policy

Bring Your Own Device (BYOD) is now being widely adopted by several organizations. With the adoption of BYOD culture, the organizations allow the users to bring their own devices. The users use the same personal device for their personal and official work. For example, a user brings his personal laptop to work. Instead of the organization spending money on purchasing the laptop, the user uses his laptop for all his official work.

With BYOD, the organizations face a security risk of data security. The users store the organizational data on their devices, putting the organization at risk if lost or stolen. However, the organizations can reduce the risk by implementing the BYOD policy, usually backed by Mobile Device Management (MDM).

The BYOD policy defines several guidelines for personal devices. Some of the key guidelines are:

- The make and models of mobile devices
- Ownership of the information stored on the mobile device – organizations still own the information
- Types of applications that can be installed on the mobile devices – mostly, application whitelisting is used to allow specific apps

MDM can be a great advantage for organizations. It can control the personal device from a security point of view, but it can also wipe the device if it is lost.



# Remote Access Policy

Data Loss  
Prevention Policy

Security Policy

Onboarding and  
Offboarding Policy

Remote Access Policy

Bring Your Own  
Device (BYOD) Policy

Acceptable  
Use Policy

Password Policy

- Is defined by an organization to allow the users to bring their personal devices for official work
- Defines the types of devices can be used
  - Models
  - Ownership of the information on personal devices
  - Types of apps used
- Can enforce the use of Mobile Device Management (MDM) to protect information in BYOD devices

# Remote Access Policy

Several organizations allow users to work from remote locations. With the pandemic, organizations had to scale up their infrastructure to allow users to work from home and connect to the network if required. To enable users to connect to the network remotely, the organizations need to implement the remote access policy.

This policy defines who can connect, how they connect, and what software they need to use. When users need to connect to the network remotely, they need to use client software. On the other end, a server software accepts, authenticates, and authorizes the remote connections. Access to the network resources is granted based on the privileges a user has.

There are several key components of a remote access policy. Some of the key ones are

- Which are the users who are authorized
- The type of remote connectivity – remote access or VPN
- Security requirements for remote connection – updated antivirus and Windows Update etc.
- Employee's Responsibilities – what are the employees supposed to do as their responsibilities
- The procedures that need to be followed for the remote connection
- Approval process – which authorizes the connection after a request for remote access is raised. It also defines where to raise the request.
- Exceptions and sanctions – What are the exceptions for remote access. For example, access allowed to a contractor because of a critical project



# Onboarding and Offboarding Policy

Data Loss  
Prevention Policy

Security Policy

Onboarding and  
Offboarding Policy

Remote Access Policy

Bring Your Own  
Device (BYOD) Policy

Acceptable  
Use Policy

Password Policy

- Is used when a user joins or leaves the organization
- Defines the processes to be followed when a user joins or leaves
- Requires some of the key tasks to be performed as part of onboarding:
  - Assigning of a system, email, and workstation
  - Paperwork completion with the HR
  - Access to the network resources
- Requires some of the key tasks to be performed as part of offboarding:
  - Handover of the system
  - Deletion of user account and email



# Onboarding and Offboarding Policy

When a user joins an organization, the onboarding process needs to be followed. In the same way, the offboarding process comes into the picture when a user leaves the organization. Both the processes are initiated through the onboarding and offboarding policy.

Onboarding and offboarding is the process that is handled by the human resources (HR) department in an organization. However, the HR department must coordinate with the IT team to ensure the smooth functioning of the onboarding and offboarding policy.

Let's look at the onboarding part of this policy. The onboarding requires several tasks to be completed that are defined in the policy. Some of the key tasks are:

- Completing the joining formalities – includes the paperwork that HR needs to complete.
- Assigning a system or a laptop, email, network account, and a workstation to the user. The HR team initiates this in most cases to the IT team. In several organizations, this is done even before the user walks in on the first day.
- Access to the network resource based on the user's profile or role within the organization

Offboarding is the reverse process of onboarding. This policy defines the tasks that must be performed to complete the offboarding process. Some of the key tasks are:

- Release of the system after ensuring complete backup
- Backup handover to the respective project or team leader
- Deletion of the user and email accounts
- Relieving letter to the user



# Security Policy

Data Loss  
Prevention Policy

Security Policy

Onboarding and  
Offboarding Policy

Remote Access Policy

Bring Your Own  
Device (BYOD) Policy

Acceptable  
Use Policy

Password Policy

- Defines the security methods that are implemented and must be enforced to protect the network, its devices, and information
- Defines the actions to be taken when a security threat occurs
- Has components, such as:
  - Purpose
  - Audience
  - Objectives
  - Responsibilities
  - Data classification
- Should be shared with all users within the organization

# Security Policy

A security policy is a document that defines the methods to protect an organization's infrastructure. It is a well-thought-through document that considers various threats and risks and then defines the security methods. It also contains the methods that should be used if a threat occurs. It takes threats that emerge from within and outside the organization into account.

The security policy considers the IT infrastructure and the physical infrastructure as well as the assets that exist within the organization. Most organizations write the security policy and then forget about it. It is a document that needs to be updated from time to time. One of the key reasons is that the infrastructure changes and therefore, the security document cannot really be used in case the threats occur. Therefore, as and when there are changes, the security policy document should be updated.

There are several components of a security policy document. Some of the key components are:

- Purpose
- Audience
- Objectives and scope
- Responsibilities
- Data Classification

The security policy document should be shared with every user in the organization. Now, not everyone in an organization is tech-savvy. For example, the HR team will not be able to understand the technical terms. Therefore, the security policy document should be written in simple plain English that is understood by everyone.



# Data Loss Prevention Policy

## Data Loss Prevention Policy

### Security Policy

### Onboarding and Offboarding Policy

### Remote Access Policy

### Bring Your Own Device (BYOD) Policy

### Acceptable Use Policy

### Password Policy

- Prevents the unauthorized sharing of information by the users
- Prevent the confidential information from going out of the network
- Has key components, such as:
  - Confidential information identification
  - Tracking and logging of information
  - Methods to be used to prevent unauthorized use and sharing of information
  - Actions to be performed in case of an attempt for an unauthorized share

# Data Loss Prevention Policy

For an organization, the danger to its data and infrastructure can emerge from outside and inside. It can put in efforts and technology to protect the data from external threats, but it is not easy to protect the data from internal threats. To handle the internal threats, organizations have started to implement the Data Loss Prevention (DLP) policy, which prevents users' unauthorized sharing of information. For example, if there is no DLP policy, the organization does not classify its data, and users can have permission on the information they should not.

The DLP policy defines the types of information. It categorizes the information and identifies the confidential information. Along with this, the policy also defines the methods for tracking and logging data usage. The other components it contains are:

- Methods that have been implemented to prevent unauthorized data usage
- If an organization has several offices, which of them are the target for the policy implementation
- Actions that must be performed for data loss prevention. For example, an alert should be sent to the administrator mobile phone.

## *TOPIC 3*

---

# COMMON DOCUMENTATION

---

# Physical Network Diagram

Baseline Configurations

Audit and Assessment Report

Site Survey Report

Wiring Diagram

Logical Network Diagram

Physical Network Diagram

- Documents the physical assets of an organization
- Is also known as network map
- Defines the physical layout of the network containing switches, routers, cables, servers, clients, VoIP phones and so on
- Helps to track the network assets and can be used to rebuild the network
- Needs to be updated as and when there are network architectural changes or devices are added or removed

Floor Plan

Rack Diagram

MDF

IDF



A network consists of switches, routers, cables, servers, firewalls, and so on. There can be several other additional components, such as VoIP phones and Wireless Access Points (WAPs). These are the physical assets of a network that are documented in the physical network diagram or network map. It defines the layout of the physical assets on the network.

Other than just defining the layout of the physical assets, organizations can also capture additional details of these assets. For example, an organization may also capture these assets' make, model, and firmware versions.

Now that you know what a physical network diagram is, why do you think it was created first place. Well, there are two key reasons. First, you know where each asset is located on the network. You would know, in seconds, where the asset is located. The second reason is that you can also find the assets for troubleshooting purposes. If there is a need to replace an older or faulty device, you can do that by tracking the device on the physical network diagram. It is mostly easy to track the firewall and routers as they are few in numbers, but what about the switches and servers. It can be difficult to track them as they might be hundreds in number. That is where you use the physical network diagram. It is also critical to understand that creating the physical network diagram is not a one-time job. Remember that your network will continue to evolve. New physical assets may be added, or older ones may be replaced or upgraded. When there are changes, you should update the physical network diagram and don't forget to add the revision information in it.

There are a few key components of a physical network diagram. An organization may treat them as an independent document, but they come in handy when referring to a physical network diagram. Let's look at them.

### Floor Plan

Your organization may be spread on to a single or multiple floors in a building. It could be possible that it is spread across multiple locations. However, what is important is the documentation of the floor(s) where your organization has the office. A floor will be divided into workstations, rooms, such as meeting and conference rooms, and so on. You will have several physical assets that might be housed in a small server room. The entire layout of the floor needs to be documented in a floor plan, which can come in handy when you need to add more physical assets or even during a disaster when you need to perform evacuation.

Let's take the example of extending the server room. You can use the floor plan to determine the room that can meet this purpose.

### Rack Diagram

A rack can house several physical assets, such as servers, switches, routers, monitors, and patch panels. You may have more than one rack. Think of a datacenter with hundreds of racks and each one housing several physical assets. How do you remember what is stored in each one of them? You need to have the rack diagrams that have a visual representation of the rack with its components. Each component is clearly labeled for easy tracking.

The rack diagram should have a visual representation of the front and back of the racks.

#### Main Distribution Frame (MDF) Documentation

Your office will have several types of wires coming in. These could be electrical wires or an Internet leased line from the service provider. Such wires are terminated in a panel that is known as the Main Distribution Frame (MDF). It is the termination point for all the cables that come into a facility or building.

#### Intermediate Distribution Frame (IDF)

From an MDF, the cables are then further distributed to one or more floors. These cables are then distributed to the IDFs that are located on different floors. For example, if there are seven floors in a building, it would have one MDF, and then each floor will have one IDF that receives the cables from the MDF. On a floor, the cables are then distributed to their appropriate locations.



# Logical Network Diagram

Baseline Configurations

Audit and Assessment Report

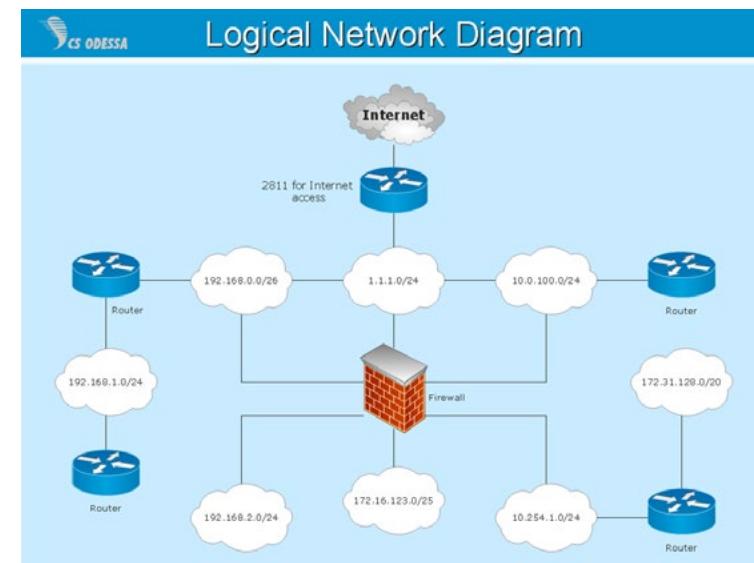
Site Survey Report

Wiring Diagram

Logical Network Diagram

Physical Network Diagram

- Defines the flow of information on a network
- Displays the communication between two or more devices
- Includes:
  - Subnets
  - Network devices
  - Routing protocols
  - Domains
  - Voice gateways
  - Traffic flow
  - Network segments



The logical network diagram is used for showing the flow of information over a network. It still shows some of the key physical assets, such as routers and firewalls. Each asset is labeled and can be marked with an IP address. With the help of a logical network diagram, you can visualize how the communication is taking place between two or more devices.

For example, let's consider that you have two offices that are connected via a site-to-site VPN. You will have this marked in the logical network diagram that displays the subnets at both the ends, routers and their details, and some information on the VPN.

You can capture information like the subnets, key network devices, such as routers, routing protocols being used, and so on.

# Wiring Diagram

Baseline Configurations

Audit and Assessment Report

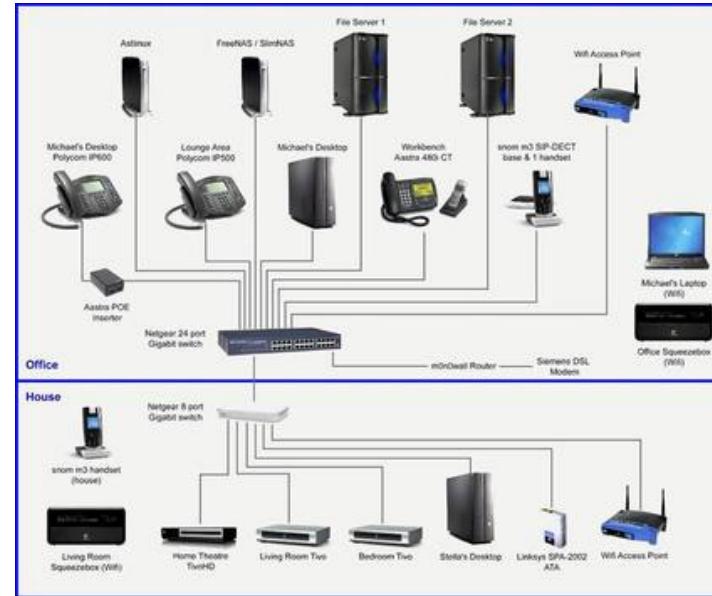
Site Survey Report

**Wiring Diagram**

Logical Network Diagram

Physical Network Diagram

- Defines the wire schema for the network
- Shows the devices that are wired up on the network
- Shows the flow of wires all over the network and their termination points
- Labels each wire or a group of wires so that they are easy to trace



Wires are an essential part of a network. There are electrical wires that power the physical devices. There are other wires, such as Ethernet, that enable communication. Even a small network can have hundreds of wires that may be used for enabling communication. Think of a large datacenter with thousands of wires. How do you track these wires? Let's say that you need to track the backbone? It can be a time-consuming task.

This is where the wiring diagram comes into the picture. It lays out the wiring schema that is used. These wires connect with physical devices like routers and switches. The wiring diagram labels each wire and shows its termination at both ends. For example, one end is the patch panel, and the other end is the router. If there are hundreds of cables, you know, the port 24 on the patch panel connects to the router by looking at the wiring diagram.

Each wire must be properly labeled. Organizations typically have a naming convention for the wires – similar to the naming convention for the physical devices. If it is not possible to label each wire, then a group of wires, let's say for a specific patch panel, must be labeled together. It is still easy to find a wire from a specific group rather than thousands of them. The labelling of the wires should then be reflected in the wiring diagram.

# Site Survey Report

Baseline Configurations

Audit and Assessment Report

**Site Survey Report**

Wiring Diagram

Logical Network Diagram

Physical Network Diagram

- Is created for a wireless network before its implementation
- Records the locations that can be used for hot spot installation
- Contains the information on:
  - Number of access points required
  - The location of installation of access points
  - Blind spots
  - Redundancy level
  - Channel Interference
  - Signal strength

Let's say that your organization uses a wired network and wants to implement a wireless network. How would you figure out where to put the wireless access points or WAPs? How many WAPs should you install? Before you proceed with installing a wireless network, you need to perform the site survey and prepare the report with its outcomes.

In the site survey, you will be able to figure out the number of WAPs, their placement, and blind spots where you think wireless connectivity will not reach or where the level of interference will be high. All this needs to be documented in the site survey report.

You will also need to include the mounting locations of the WAPs as well as the cable path. Do you need to know how the WAPs are going to be powered on? Are there electrical sockets available, or the WAPs are going to be Power-over-Ethernet (PoE) enabled? You also need to include the level of WAP redundancy. For example, if there is no WAP redundancy, the failure of one WAP can turn that particular location into a blind spot. You will also need to include the signal strength.

There are automated tools that can provide all this input without having to perform actual tests.



# Audit and Assessment Report

Baseline Configurations

Audit and Assessment Report

Site Survey Report

Wiring Diagram

Logical Network Diagram

Physical Network Diagram

- Is created after audits based on the security policies and processes are performed
- Captures the audit and assessment output in a defined format
- Is visited repeatedly until all non-conformances or observations are closed
- Are recorded as evidences

With the implementation of various types of policies, it is essential and critical for an organization to ensure that they are implemented properly and are providing outcomes as they should. To ensure this, organizations conduct audits of their security policies. Assessments could be of the various servers and applications. Penetration testing and vulnerability assessments are usually done to know the security weaknesses that can be exploited. The outcomes of the audits and assessments are recorded in the audit and assessment reports.

Each organization usually defines a format for the outcome, which is a standard one. There can be, however, different formats for audits, vulnerability assessment, and penetration testing. Organizations that hire external agencies for these tasks may use the format that has been provided to them.

After the reports are ready, they are visited to close the issues that have been reported. Next time the audits or assessments are performed, the previous reports may be visited to see the closure of reported issues. In a way, the reports serve as evidence that the issue was reported.



# Baseline Configurations

## Baseline Configurations

Audit and Assessment Report

Site Survey Report

Wiring Diagram

Logical Network Diagram

Physical Network Diagram

- Defines the normal performance of a system, application, or even the entire network
- Requires setting the performance thresholds
- Are used in benchmarking the system, application, or network performance later
- Can be altered if required
  - When the configuration changes have taken place
  - When the number of devices have changed

The network, servers, and applications are expected to have normal behavior, which is the device's performance. A baseline can be used to define normal behavior. For example, you expect a server's CPU utilization to be always less than 70 percent. You consider that as normal behavior. Similarly, you define the normal behavior for the memory, hard drive, and network. You set the normal functionality metrics for each, such as memory utilization, to be less than 50 percent. These functionality metrics are part of a baseline.

After defining a baseline, you benchmark the performance. If there is a deviation, such as high CPU utilization, you can consider the performance bottleneck. Whenever you create a baseline, the server or application, whichever is the baseline's subject, has a certain configuration. If the configuration changes, you must consider creating the baseline once again.

Similarly, if you have created a baseline for network performance and several devices have changed, let's say more have been added, there will be an obvious deviation in the network performance. You should re-create the baseline.



## TOPIC 4

# COMMON AGREEMENTS

# Non-disclosure Agreement (NDA)

Memorandum of  
Understanding (MoU)

Service-level  
Agreement (SLA)

Non-disclosure  
Agreement (NDA)

- Is used for protecting the confidential information when shared with users or third-parties
- Is signed between two parties:
  - The recipient of the information needs to safeguard the information
  - The recipient must remove the information after the project competition
- Can be:
  - Unilateral
  - Bilateral
  - multilateral

An organization often works with contractors, vendors, and even other organizations. It might have to share proprietary or confidential information to execute a specific project or complete a task. The organization needs to put the Non-disclosure Agreement (NDA) in practice. An NDA is used before sharing any confidential or proprietary information with a second party. The NDA intends to protect against the misuse of the information being shared.

The recipient of the information is expected to sign the NDA and ensure that it is safeguarded by all means. As and when the project or the task is completed, the recipient, the second party, is expected to remove or delete the information in a secure manner.

An NDA document has several components, which are:

- Name of the parties involved – organization and the second party
- Definitions of confidential and non-confidential
- Information sharing restrictions
- Responsibilities of both the parties
- Penalties for NDA violation
- Disposal of information
- Duration of NDA

NDAs can be categorized into three types:

- Unilateral: Involves two parties. One party shares the information with the second party.
- Bilateral: Involves two parties that share information.
- Multilateral: Involves more than two parties. One party shares the information, whereas the remaining parties are recipients of the information.

# Service-level Agreement (SLA)

Memorandum of  
Understanding (MoU)

Service-level  
Agreement (SLA)

Non-disclosure  
Agreement (NDA)

- Involves a service provider and a service consumer
- Defines the parameters and standards for the services to be provided by the service provider
- Defines the measurable performance characteristics for the service provider
- Contains components like:
  - List of services being provided and their scopes
  - Performance metrics – must include the response and resolution time
  - Roles and responsibilities of the parties involved
  - Penalties for SLA violations
  - In-scope and out-of-scope services

An organization may hire a vendor to perform a certain task, a project or maybe perform hardware maintenance. The vendor is expected to provide services to the organization. These services are mentioned in a Service-level Agreement (SLA) document, which defines the measurable parameters for measuring the services being provided.

Let's take an example of an organization that has hired a vendor for hardware maintenance. You expect the faulty hardware to be replaced within 24-hours. You need to define this in the SLA document.

SLAs should always be measurable. It should not be something like "Faulty hardware must be replaced as soon as possible." Now, there is no concrete definition for "as soon as possible". Therefore, putting a time makes it measurable.

A typical SLA document would contain the following components:

- List of services being provided and their scopes
- Performance metrics – must include the response and resolution time
- Roles and responsibilities of the parties involved
- Penalties for SLA violations
- In-scope and out-of-scope services



# Memorandum of Understanding (MoU)

Memorandum of  
Understanding (MoU)

Service-level  
Agreement (SLA)

Non-disclosure  
Agreement (NDA)

- Is a non-legal document between two parties
- Is often used as a starting point of relationship between two organizations
- Defines the responsibilities of two or more parties involved
- Defines the:
  - Scope of the project
  - Goal of the project
  - Roles and responsibilities of each party

A memorandum of understanding (MOU) is a non-legally binding document between two or more parties. In most cases, there are two parties involved. However, it is possible to have more than two parties be part of the MoU. An MoU is often used as a starting point of negotiation between two parties. For example, two countries signed an MoU for a student exchange program.

Just like any other agreement, an MoU lists the responsibilities of each party. Each party is expected to perform as per the responsibilities listed in the MoU.

Like any other agreement, the MoU document also has several components, such as the parties' names, project name and scope, the outcome or goal of the MoU, and the responsibilities of the involved parties.



# Summary

- Plans and procedures
- Hardening and Security Policies
- Common Documentation
- Common Agreements



That's the end of the lesson.

Here, we covered:

- Plans and procedures
- Hardening and Security Policies
- Common Documentation
- Common Agreements



**NEXT TOPIC**

---

# HIGH AVAILABILITY AND DISASTER RECOVERY

---

Lesson

3

---

# High Availability and Disaster Recovery

- 1 — Welcome to the lesson 3 of Module 3. In this lesson, you will learn about the:
  - 2 — High Availability and Disaster Recovery
- 



Network Fundamentals

# Agenda

- Load balancing
- Multipathing
- Network interface card (NIC) teaming
- Redundant hardware/clusters
- Facilities and infrastructure support
- Redundancy and high availability (HA) concepts
- Redundancy and high availability (HA) concepts

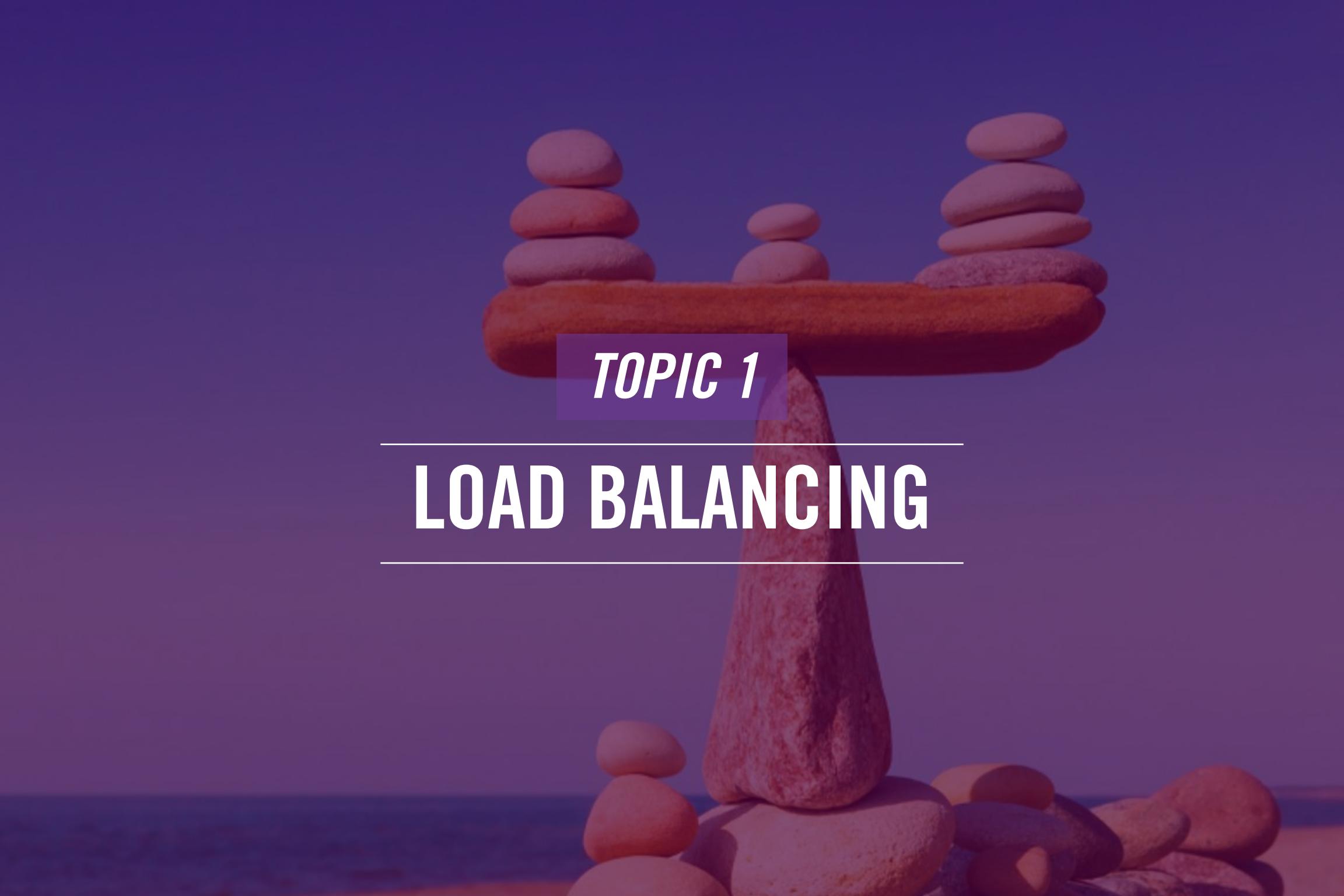


Hi, welcome to COMPTIA Network+ Course

In this lesson, we will talk about:

- Load balancing
- Multipathing
- Network interface card (NIC) teaming
- Redundant hardware/clusters
- Facilities and infrastructure support
- Redundancy and high availability (HA) concepts
- Redundancy and high availability (HA) concepts



The background of the slide features a photograph of several smooth, reddish-brown stones balanced in a cairn-like structure on a sandy beach. The stones vary in size and shape, with some being flat and others more rounded. They are set against a dark blue sky and a dark ocean. The lighting suggests it is either sunset or sunrise, casting a warm glow on the stones.

## *TOPIC 1*

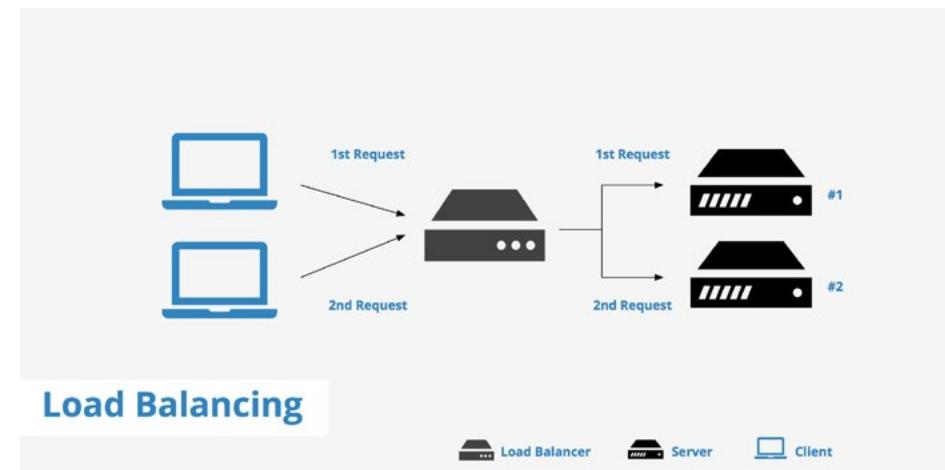
---

# LOAD BALANCING

---

# Load Balancing

- Distributes incoming network traffic
- Maximizes speed and efficiency
- Can be performed using hardware or software load balancers
- Can be performed at various locations in a network:
  - Between the webserver and the users
  - Between the webserver and application servers
  - Between the application servers and databases



Load balancing in the networking world is all about distributing the incoming traffic to one or more servers. When load balancing is configured, one server does not have to bear the complete load. Using different methods, load balancing can automatically decide the server to which the traffic needs to be sent, which eventually eases the load on the other server if it is already busy. With the load distribution, the servers can perform with speed and efficiency and handle the load they already have. For example, let's consider that you have two web servers that are configured with load balancing. When traffic comes, it does not directly hit the webservers. It lands with the load balancer that smartly distributes it to the next server or server with minimum load – it depends on the algorithm you use. With this method, both the servers perform with equal efficiency.

Let's talk about some of the most commonly used algorithms. Round-robin is one of the most widely used algorithms in load balancing. It shares the load in sequence. For example, it will send the load or traffic to the first server, second, and third server. If there are no more servers, it returns to the first server and continues in the same sequence.

Load balancers can be hardware or software-based. The hardware load balancers are devices that handle the incoming traffic and appropriately distribute them to the available or next server in the queue. The software load balancer is an application that can be used to handle the role of the hardware load balancer. There is no special device that you have to procure. Another most commonly used algorithm is about sending the load to the next available server. For example, if two out of three servers are busy performing some tasks, the load is distributed to the third server.

Depending on the network architecture, the load balancers can be configured in different ways, such as:

- Between the web server and the users
- Between the webserver and application servers
- Between the application servers and databases



*TOPIC 2*

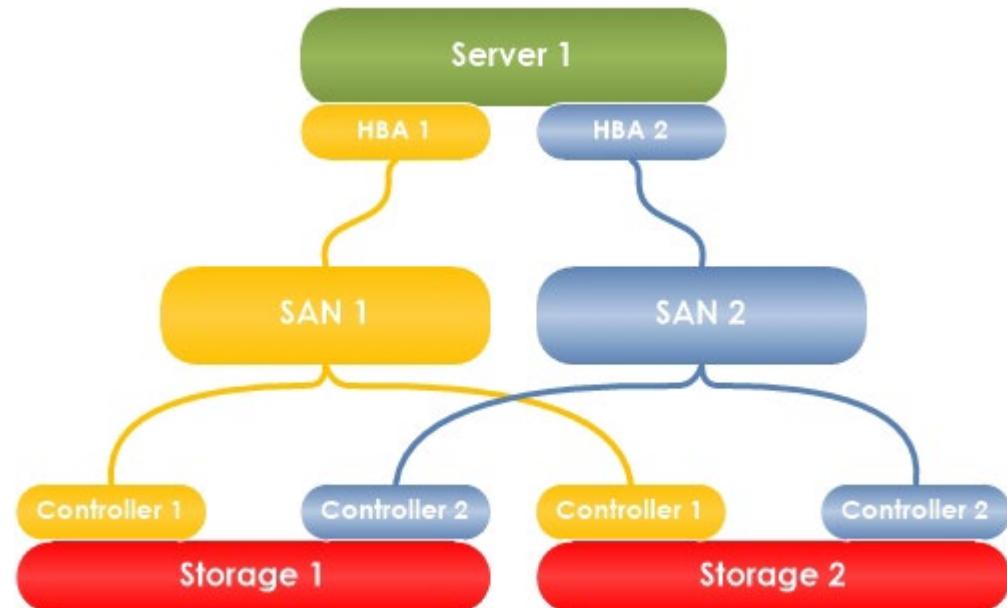
---

# MULTIPATHING

---

# Multipathing

- Automatically directs communication between a client and remote storage to alternative paths during failures Storage clients (nodes) access remote disks
- Each node can have multiple physical connections to the disks
- In the event of failure, the operating system transparently fails over to the other connection



Organizations usually have storage devices and the clients that connect to them. In the usual configuration, the clients have one single connection to the storage device(s). If the single connection goes down, the clients cannot reach the storage device(s). This is where multipathing features in. It brings in the concept of path redundancy between the clients and the storage devices. There is one primary path that the clients use to connect to the storage device. Then, there is an alternate path. If the primary path goes down due to some reason, then the alternate path is used.

You can have one SCSI hard drive connects to at least two SCSI controllers in the same system. The SCSI controllers are connected to the storage devices forming two paths. If the first controller has an issue or the path to the storage device is not available, then the alternate controller is used for communication.

In multipathing, the user is not aware of the path that is taken to the storage device. It is the operating system's job to quietly switch to the alternate path if primary is not available.

## *TOPIC 3*

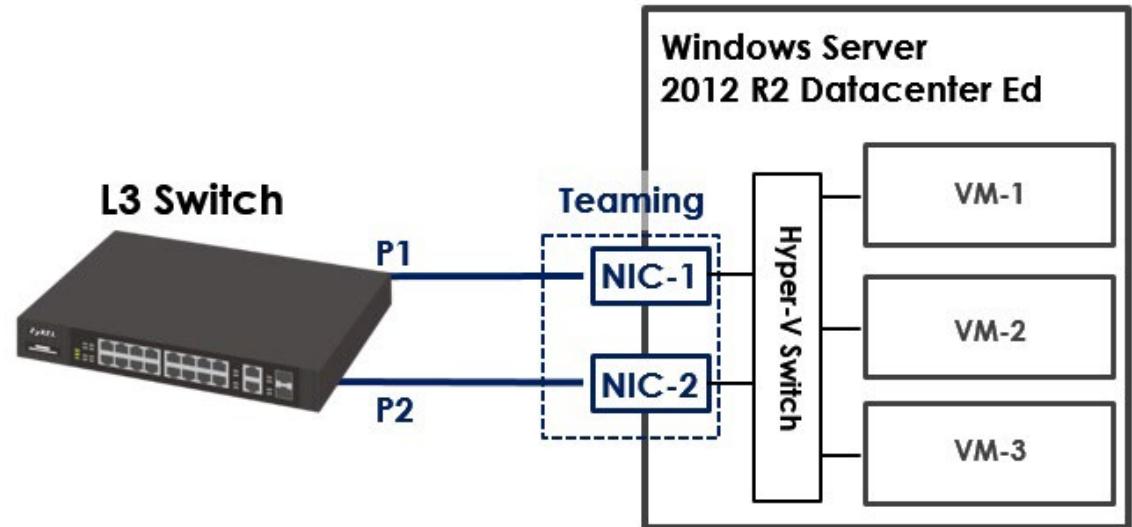
---

# NETWORK INTERFACE CARD (NIC) TEAMING

---

# Network Interface Card (NIC) Teaming

- Enables multiple physical network adapter cards to work as a single logical interface
- Works with a shared IP address
- Provides benefits of:
  - Load balancing
  - Fault tolerance
- Can work in active-active or active-passive mode

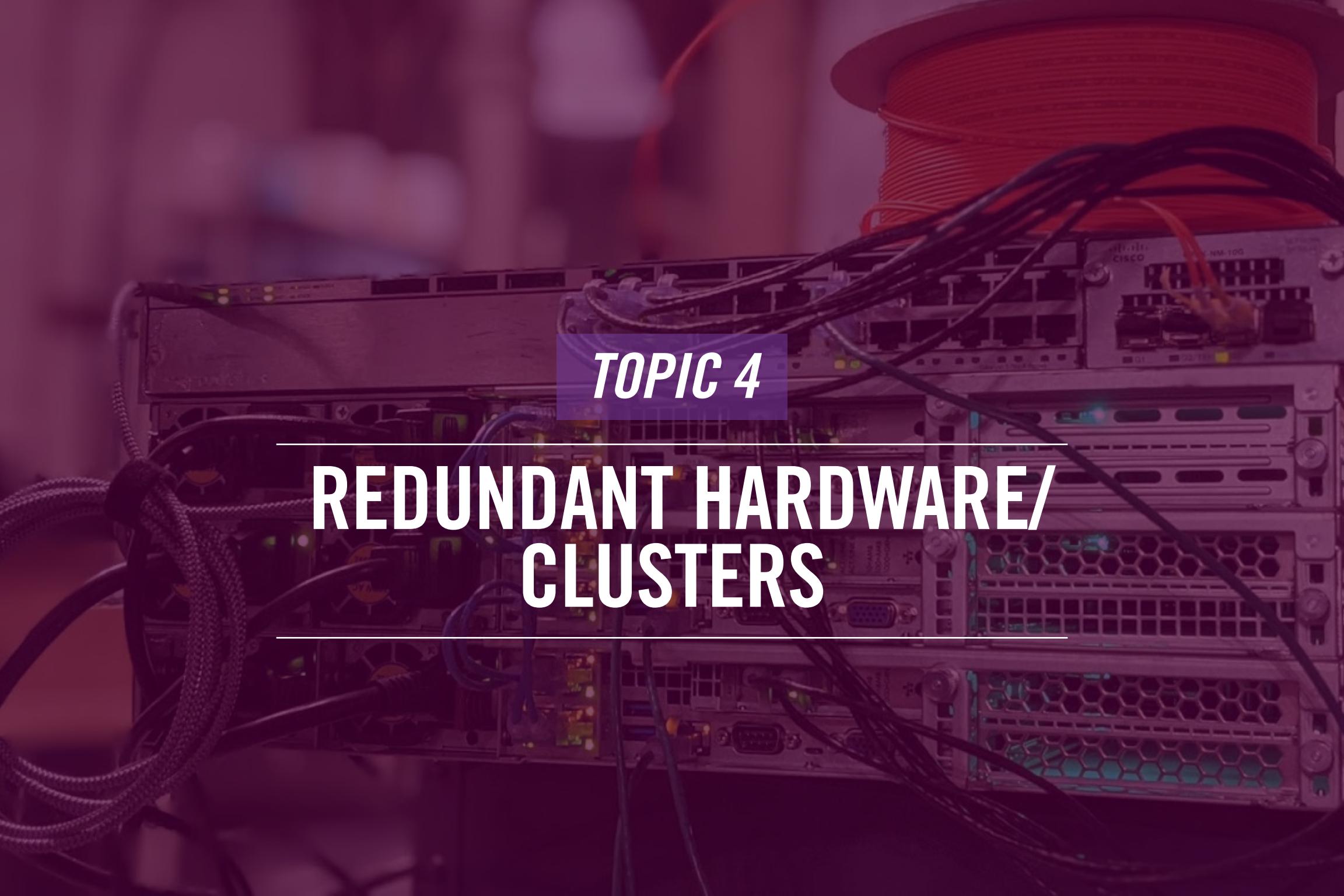


In the previous slide, you looked at the issue of having a single NIC in a webserver. This can be solved by using NIC teaming, which configures multiple NICs to work as a single NIC. When you configure NIC teaming, the webserver functions and continues to provide services to the client even if a NIC fails. You combine multiple physical NICs into a single logical NIC that the clients see. They are unaware of the NIC teaming at the backend that is configured. All NICs are participating in NIC teaming use the same IP address. For example, if NIC1 has an IP address of 192.168.1.10, the second NIC will also have the same IP address.

With the NIC teaming configuration, you get several benefits. The first benefit is load balancing. The outgoing traffic is sent through all the available NICs. The load is not only on one single NIC. The second benefit is fault tolerance. If one NIC malfunctions or has an issue with it, then the traffic is sent through the second NIC.

NIC teaming can work in two different modes:

- Active-active: In this configuration, both the NICs are working and perform load balancing of the traffic.
- Active-passive: In this configuration, one NIC is active, and another one is passive. The active NIC is used, and when the active NIC goes down, the passive one becomes active.



*TOPIC 4*

---

# REDUNDANT HARDWARE/ CLUSTERS

---

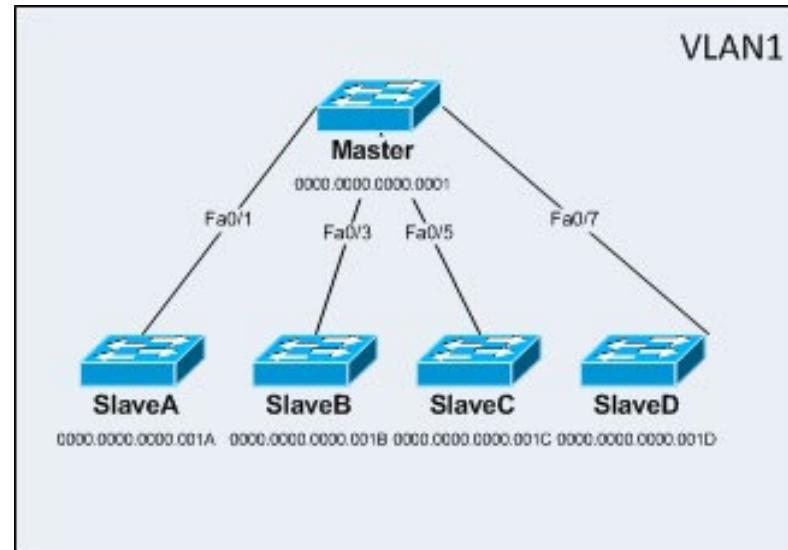
# Redundant Hardware/Clusters

- Is a group of servers, switches, or any devices that form a group to act like a single device or system
- Is used for fault tolerance and redundancy
- Performs automatic failover to another server or device
- Can cluster switches, routers, and firewalls along with servers

Switches

Routers

Firewalls



When you are working with single hardware, a server, a minor technical issue can make the server non-functional or unavailable for the users. To avoid a single point of failure, you can group similar networking devices, like servers and switches, into a group to make them function as a single unit. For example, you can group two servers in a cluster to perform a specific function like hosting a web application. The end users do not see two servers. They see a single web server that is a logical one. However, it does not make any difference to the users as they get to access the web application.

When you have a cluster, you have two key benefits. The first benefit is fault tolerance. A single server in the cluster continues to function. If one of the servers in the cluster fails, the other server continues to function. The second benefit is redundancy. Failure of one server does not make the web application non-functional.

Depending on the cluster, both the servers can be active at the same time. You can also have active and passive configurations. In this configuration, one server is active and serving the requests. However, when the active server goes down, the passive server takes over. Clustering can be complex to configure. You need to know the type of cluster you are configuring – active/active or active/passive.

Up till this time, you have heard of servers in the examples. However, you can also cluster switches, routers, and firewalls. For example, you have a firewall configured at the entry point of the network. One firewall is configured in the active mode and another one as passive. The same can be done with the routers. Such configuration ensures that the entry point is always guarded even if there is a firewall failure.



**TOPIC 5**

---

# FACILITIES AND INFRASTRUCTURE SUPPORT

---

# Facilities & Infrastructure Support - UPS

Fire Suppression

HVAC

Generator

Power distribution units (PDUs)

**Uninterruptible Power Supply (UPS)**

- Is also known as battery backup
- Provides power backup when the main source of power fails
- Keeps the systems running in an event of power failure
- Provides power backup depending on its capacity



UPS or Uninterruptible Power Supply is one of the essential components of a data center. It is also known as the battery backup. The data centers require a lot of electricity to run. This is done through the primary source of electricity that is coming in. However, if the primary electricity source fails, you need to have something as a backup to keep the data center running. A UPS performs this job. In a power failure, a UPS takes over and provides the power to the components within the data center.

UPS can come in different sizes. For example, you can buy a UPS for a single system or a UPS to support the entire data center. Therefore, when planning a data center, calculate the approximate electricity load and accordingly plan for the UPS. The capacity of the UPS will determine the amount of backup (time) it can provide to the data center equipment.

A UPS can be a standby, line-interactive, or double conversion. Ensure that you know what your need is. For example, a standby UPS is mainly used when there is an issue with the power, such as a blackout or voltage surge. A standby UPS can handle it on its own. The line-interactive UPS is designed to correct power issues, such as brownouts and swells. A double-conversion UPS cleans the power before supplying it to the equipment. They are mainly used with mission-critical appliances, such as high-end servers and storage devices.

# Facilities & Infrastructure Support - PDUs

Fire Suppression

HVAC

Generator

Power distribution units (PDUs)

Uninterruptible Power Supply (UPS)

- Distributes the power from the main power supply or even a UPS to the network devices and appliances
- Sources the power from a single source and distributes
- Can be installed in different locations, such as data centers and network closets



The main job of the Power Distribution Units or PDU is to distribute power to multiple devices. There is usually one power source, let's say to a server rack, but then there are several devices to power on. You need to use the PDU to accept the incoming power and then make it available to the devices housed in a server rack or a network closet.

The power can be sourced from different sources, such as a UPS, a generator, or the main power line, and then needs to be distributed to the servers or the devices within the data center.

The PDUs can be located in different places in a data center. PDU can take the main source of power to distribute it to the rest of the racks that also have smaller PDUs installed.

# Facilities & Infrastructure Support-Generator

Fire Suppression

HVAC

Generator

Power distribution units (PDUs)

Uninterruptible Power Supply (UPS)

- Provides the power backup support a datacenter or a building
- Plays a key role in running the data center up and running in case of a power failure
- Can work as a backup to the UPS, which acts as the primary backup to the main power
- Requires several factors to be considered before deployment:
  - Which type?
  - Which size?
  - Which deployment location?
  - How long can it run?

Like the UPS, generators also provide a backup power supply to a data center or a building. Organizations usually have generators as the last power backup method. First, there is primary power, then UPS, and then the generators. Unlike UPS, generators need to be powered on, and therefore, they are not the first backup to the main power. If the main power fails, there will be a complete shutdown in the building, including the data center. This leads a downtime. Therefore, you always have the UPS as the main power back up and then the generators as the backup of the UPS.

When purchasing a generator for the building or data center, you need to consider the following factors, such as:

- Which type do you need?
- What size do you need to support the size of the infrastructure?
- Where is the generator going to be deployed?
- For how long is the backup required from a generator?

Depending on the answers to some of these questions, you need to purchase the generator.



# Facilities and Infrastructure Support - HVAC

Fire Suppression

HVAC

Generator

Power distribution units (PDUs)

Uninterruptible Power Supply (UPS)

- Stands for Heating, Ventilation, and Air Conditioning
- Are required in the data center and other facilities to control the environment – temperature, humidity, and air flow
- Are critical part of a data center – as critical as other hardware and devices, such as servers
- Requires careful planning for its implementation:
  - The location of the devices and racks
  - Location of the electrical switches
  - Temperature and humidity in the datacenter

HVAC is an acronym for heating, ventilation, and air conditioning. Data centers are usually cramped with a lot of racks, servers, and networking devices. You need to have an appropriate ambiance consisting of air conditioning, heating, air filtering, and ventilation to make the device perform properly.

HVAC planning is a critical part of a data center – as critical as the devices in the data center. For example, excessive heat can cause the servers and devices to reboot. It needs to be controlled with proper ventilation. On the other hand, if there is high humidity, it can cause corrosion problems. Low humidity can generate an excessive amount of static current that can cause damage to the devices that are running.

Since the data centers are closed environments and have many devices continuously generating heat, if the heating is not controlled properly, it can cause severe issues with the devices. For example, if a server heats up, it might just start rebooting. Therefore, you need to ensure that heat does not accumulate in the data center. This requires a lot of data center planning, such as the placement of the server racks. The backside of one rack should not be facing the front side of another rack. The racks should be facing each other so that the heat generated from one rack is not absorbed by the servers in another rack.

You need to plan for the electrical switches so that the electricity distribution is equal and there is no load on a single electrical panel.

Finally, the temperature needs to be controlled to control high heat or high/low humidity.



# Facilities and Infrastructure Support – Fire Suppression

## Fire Suppression

### HVAC

### Generator

### Power distribution units (PDUs)

### Uninterruptible Power Supply (UPS)

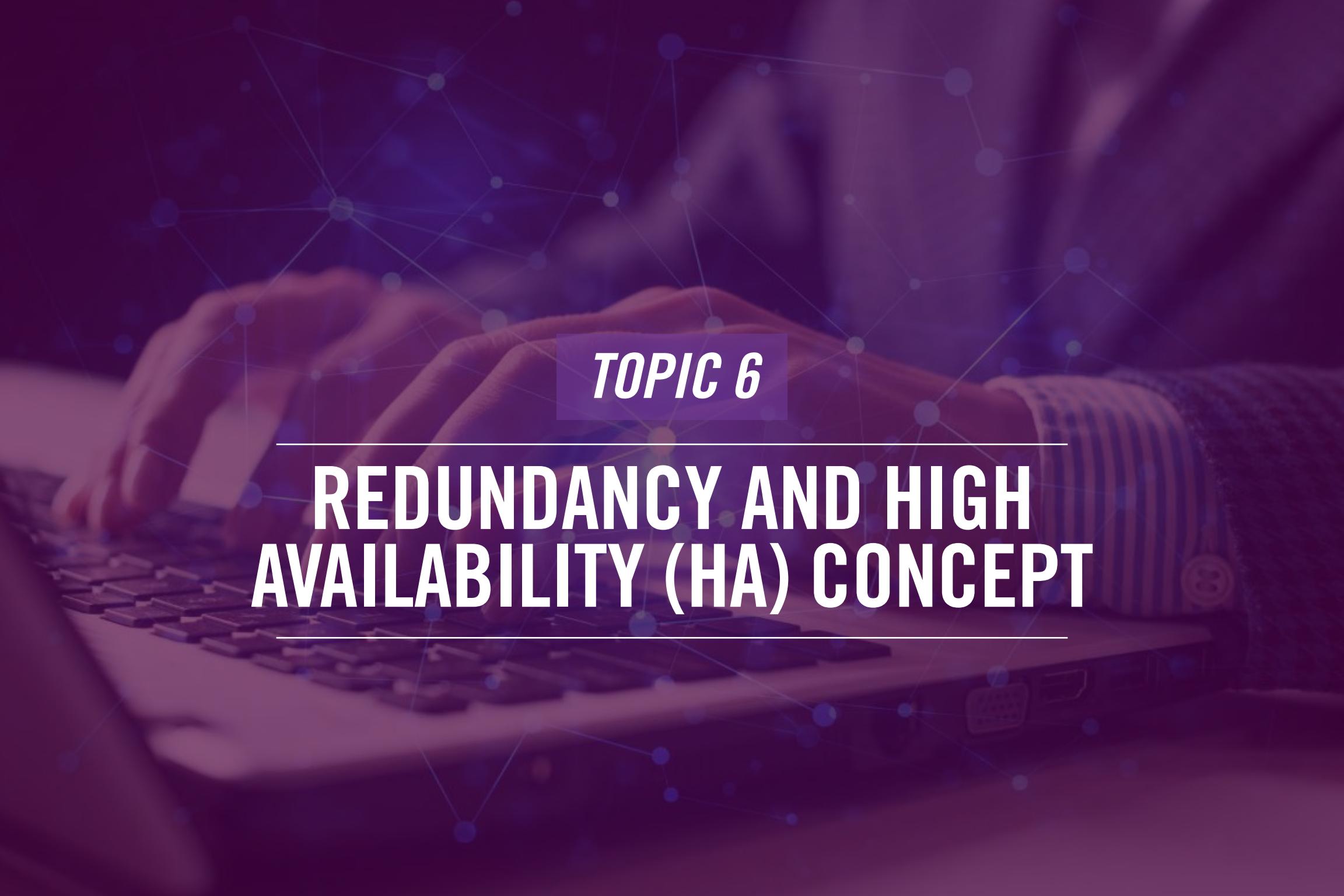
- Is required to control fires in a datacenter or building
- Can be performed by different types of agents, such as:
  - Gaseous
  - Chemical
  - Foam
- Needs to be designed and installed for:
  - Building
  - Room
  - Rack

Fires can break out anywhere and anytime if their protection is not planned. Even if a fire breaks out, you need to have fire extinguishers to control the fire. However, with the size of the data center and the building, it is better to use fire suppression systems, which can be of different types. There are fire extinguishers that release gases, chemicals, or foams. In the data center, it is recommended to use the fire suppression system, FM-200, which is considered safe for the devices within the data center.

Fire suppression systems should be planned for the building, rooms, and racks. The building-level fire suppression system protects the entire building. You also need fire suppression systems for the data centers, which need to be NFPA 75 - Standard for the Fire Protection of Information Technology Equipment or NFPA 76 - Standard for the Fire Protection of Telecommunications Facilities compliant.

Finally, you need to have the rack level fire protection, which is the automatic fire suppression system that detects and suppresses the fire before it spreads.





*TOPIC 6*

---

# REDUNDANCY AND HIGH AVAILABILITY (HA) CONCEPT

---

# Recovery Sites - Cloud

Cold

Warm

Hot

Cloud

- Is an Infrastructure as a Service (IaaS) solution
- Has the data backups and critical servers up and running
- Is part of the Disaster Recovery Planning (DRP)
- Requires minimum up time to switch from the main site
- Can be scaled up in minutes

A cloud environment can be configured to work as a recovery site. It can be a replica of the on-premises site. You have the complete site replicated but in the cloud environment. An organization that cannot afford or does not want to spend much money setting up a complete replica of the existing site can use the cloud site as a good alternative. It is cheaper and cost-effective.

An organization has data backups and critical servers running in the cloud environment. Some organizations may even choose to replicate the entire infrastructure.

One of the key benefits of having a cloud site is that you need minimum time to switch over to it in case of a disaster. You also spend relatively less amount of money. Therefore, the organizations mostly make a cloud site a part of their DRP or Disaster Recovery Plan.

Another key benefit is that you can scale up the cloud site within minutes without waiting for the procurement of hardware or software.



# Recovery Sites - Hot

Cold

Warm

Hot

Cloud

- Is a mirror of the main network infrastructure
- Contains all required equipment including servers, power, systems, and Internet connectivity
- Replicates the data asynchronously
- Is used for immediate switch over when a disaster occurs
- Is expansive to implement
- Is used for mission-critical servers and applications

Hot sites are fully functional sites that are a replica of the main network infrastructure of an organization – something like a mirror image. You have everything into a hot site, including your servers, data, internet connectivity, and other devices.

The data is asynchronously replicated to the hot site. You are replicating the data every few seconds or maybe after every minute. This means that even if you switch over to the hot site, you lose only a few minutes of data – the data created after the last replication.

As and when a disaster strikes, you have the hot site functional within minutes. Since this is a replica image, you don't have to put any effort into making it functional.

Hot sites are expansive to implement. Since they are replica images of the current site, they require the same infrastructure – this means a lot of money needs to be spent. Because of the high-cost factors, organizations usually use it for replicating mission-critical infrastructure.



# Recovery Sites - Warm

Cold

Warm

Hot

Cloud

- Is similar to the hot site but with less recent data
- Has the required hardware like servers
- Requires the restoration of recent data to make it functional
- Takes a few hours before it can be ready
- Is mainly used for non-mission critical applications and servers

A warm site is pretty much similar to a hot site but with less recent data. You need to restore the most recent version of data to make the warm site functional. Like servers, applications, and Internet connectivity, the rest of everything is in a place like the hot site.

Restoring the data is a time-consuming task, and therefore, the warm site is not fully functional without putting in several hours of work. This is because your data is not replicated in the asynchronous mode to the warm site.

The warm site is mainly developed for non-critical applications and servers that do not require immediate switch over from the main site.



# Recovery Sites – Cold

Cold

Warm

Hot

Cloud

- Are the sites with least infrastructure when compared with warm or hot site
- Are easiest to implement
- Are less costly when compared with warm and hot site
- Requires a few days to become functional

Cold sites are equipped with the least infrastructure when compared with warm or hot sites. You need to re-create your original site to make the cold site functional. This means that the IT team needs to spend several days to bring the cold site up. In a real sense, sometimes the cold sites are nothing but facilities with power supplies and bare minimum hardware.

A cold site is the easiest to implement. As stated earlier, there is bare minimum hardware, and therefore, they can be set up quickly.

They are also cost-effective as they do not require much money to be functional. However, when a disaster strikes, the IT teams have to spend several days to get them functional – more like setting up a new site altogether.



# High Availability Configurations – Active/active

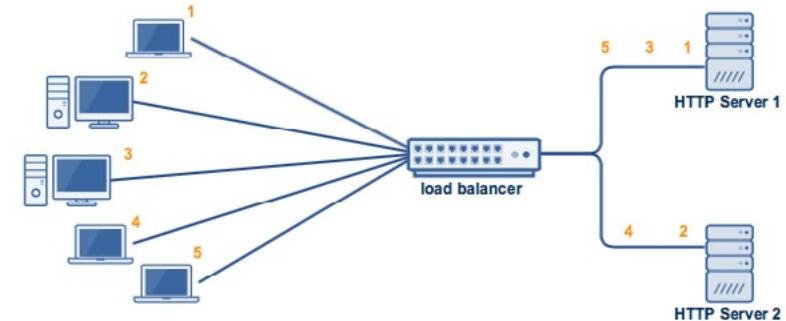
Diverse Paths

Multiple Internet Service Providers (ISPs)

Active-passive

Active-active

- Requires minimum two nodes with the same configuration
- Has both the nodes running at the same time
- Uses both the nodes for load balancing and redundancy
- Makes the client see it as one server
  - Works with an algorithm like round robin to distribute load
  - Keeps the process transparent to the clients



You learned about the cluster previously in this lesson. When you refer to the active-active cluster, it requires a minimum of two nodes to be functional. Both the nodes must have the same configuration because they will act as a single logical node. In the active-active configuration, both the nodes are up and running in parallel.

Because both the nodes are running in parallel, they provide load balancing and redundancy. If one of the nodes fails, the other nodes take over. Similarly, they also share the load.

The clients, the users at the other end, do not know whether one node is down or not. This is because a logical node is used as a front-end of the cluster. When it comes to loading sharing, the cluster can use the algorithms like round-robin, or the load can be shared with the server with less load. Whichever algorithm is being used, the clients never get to know about it, and the entire process is transparent to them.

# High Availability Configurations- Active/Passive

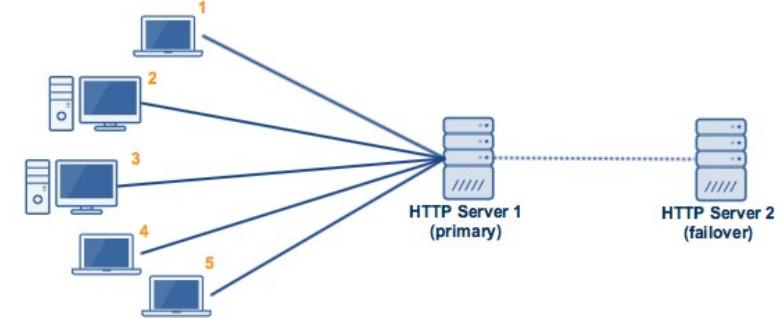
Diverse Paths

Multiple Internet  
Service Providers (ISPs)

Active-passive

Active-active

- Requires minimum of two nodes
- Has one active and one passive node
- Uses passive node as an active node when the primary node is unavailable or goes down
- Requires the changes made to the active node to be replicated to the passive node
  - the configuration must be same



[Active-Active vs. Active-Passive High-Availability Clustering \(jscape.com\)](#)

Like the active-active configuration, the active-passive configuration also requires a minimum of two nodes to make a cluster. If there are two nodes, one node is always active, and the other is always passive.

When the active node runs into a problem or goes down, the passive node becomes the active node. At the same time, the existing active node becomes the passive node. They switch their roles. Before the passive node becomes the active node, it needs to have all the changes from the existing active node to be replicated. Once all the changes are replicated, it then becomes the active node. For this activity to take place, both the nodes must have the same configuration.

# High Availability Configurations – Multiple ISPs

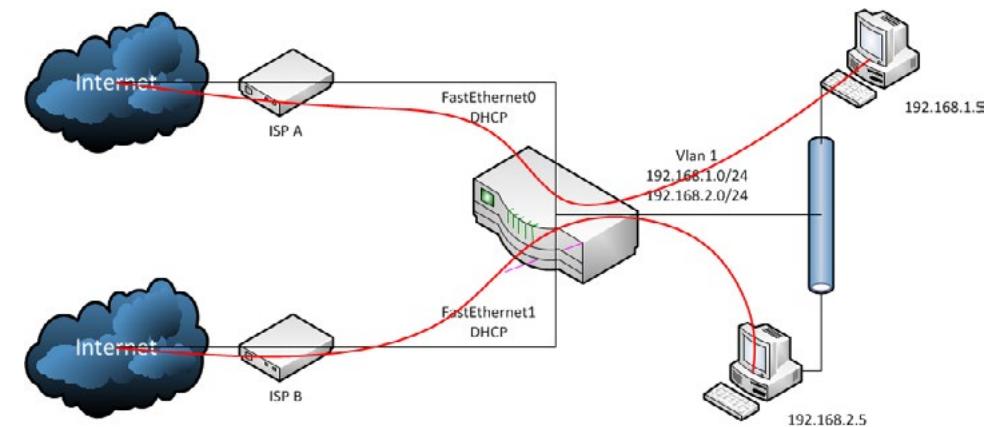
Diverse Paths

Multiple Internet Service Providers (ISPs)

Active-passive

Active-active

- Help to build redundancy in the infrastructure
- Requires one ISP to be the primary and other to be the secondary or backup
- Can also be configured for load sharing



Internet is crucial to almost all organizations for running their business operations. However, most organizations work with just one Internet connection from one Internet Service Provider (ISP), which often becomes the single point of failure. If the Internet connectivity goes down, the organization's work comes to a halt. To resolve this issue, the organizations take at least two Internet connections from different service providers. They use these connections for redundancy. If one connection goes down, the second connection from a different ISP is used. When used for redundancy purposes, one connection is typically the primary and another one as secondary.

Both the connections can also be used for load sharing. The load can be distributed to more than one Internet connection to ensure that one is not overloaded.

# High Availability Configurations – Diverse Path

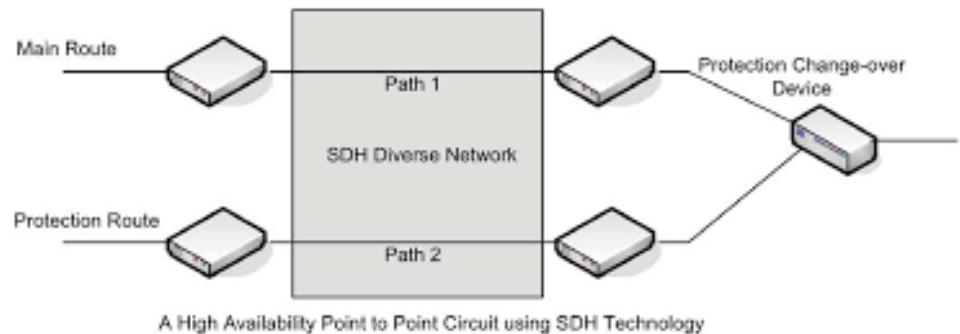
## Diverse Paths

Multiple Internet Service Providers (ISPs)

Active-passive

Active-active

- Uses an alternate path for connectivity
- Uses geographically laid different path that serves as an alternate path



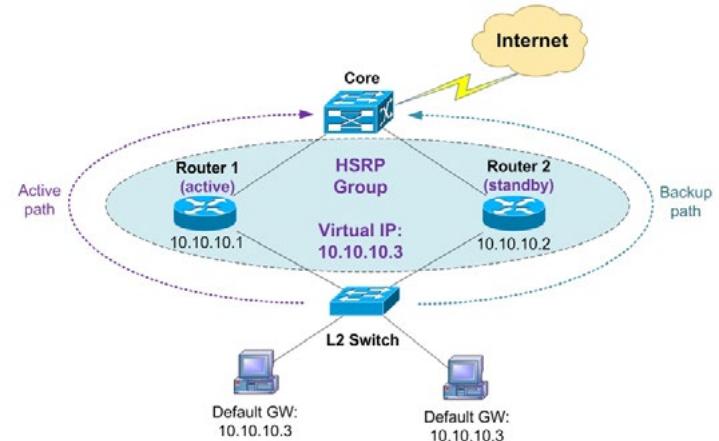
When an organization takes more than one Internet connection from different ISPs, there are alternate connectivity paths. Typically, most of the ISPs use the same geographical path for Internet connectivity. So, if one path has trouble, all the ISPs may get impacted. To resolve this problem, you should ensure that you insist on using a different geographical path from the second ISP. This can help you build redundancy, and the second path is the diverse path. If the primary path has issues or technical challenges, the second path can be used.

# Recovery Protocols - FHRP

VVRP

FHRP

- Creates redundancy for the gateway
- Allows the backup gateway to take over when the primary one fails
- Requires at least two routing capable devices, such as routers



All networks, in most cases, operate with one gateway. It could be the entire network or just the network segment – they work with one gateway. However, if the gateway is down, the network segment or the entire network comes to a halt. The users within the segment cannot communicate with the other users. If the network gateway is down, the network users cannot communicate with the rest of the world – the Internet.

The First Hop Redundancy Protocol or FHRP allows a layer 3 device, such as a router or switch, to act as a backup gateway. If the primary gateway goes down, then the backup gateway takes over. In this manner, the gateway continues to function without any reconfiguration at the client end.

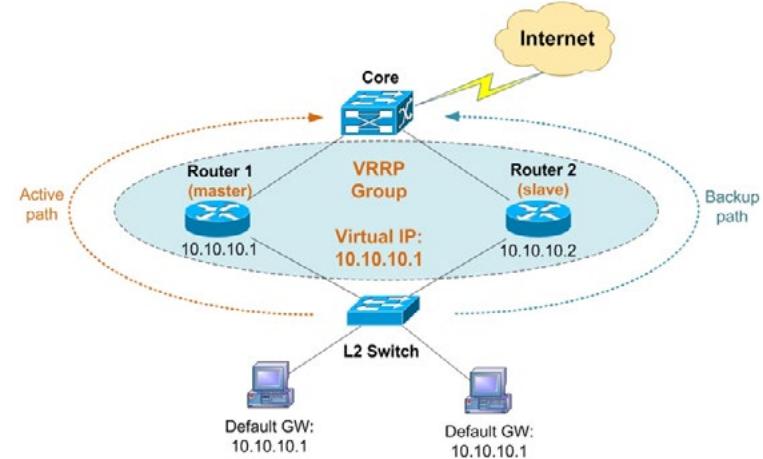
You need to have at least two routing-capable devices, such as routers, to make this happen.

# Recovery Protocols

## VVRP

## FHRP

- Creates a virtual router using two physical routers
- Create a VVRP group that contains the physical routers
- Assigns the same virtual IP address and MAC address to all routers in the VVRP group
- Has one master and one backup router



Coming back to the scenario of using a single router serving as the gateway. If it fails, the network loses connectivity with the outside world. You can use the Virtual Router Redundancy Protocol or VVRP to create a virtual router with the two physical routers.

You need to create a VRRP group that contains both routers. Each of the routers needs to have the same MAC address and the IP address. One of the routers becomes the master router, and the second router becomes the secondary router, also known as the backup router. The master router plays the role of handling the communication by sending and receiving packets. The backup or secondary router waits in the passive mode. It only acts when it becomes the master router.

If the master router becomes unavailable for some reason, the secondary router takes over the role of the primary router. This enables redundancy amongst the routers because for the users, one of the routers in the VVRP group is always available, and users do not have to make any configuration changes.

# High Availability Measurements - MTBF

MTFB

MTTR

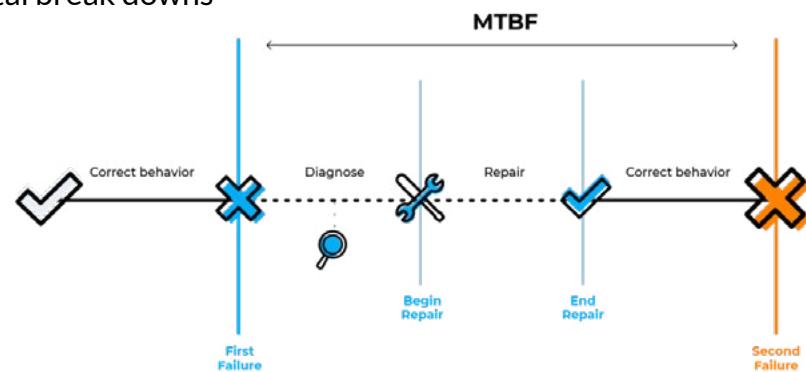
- Stands for Mean Time Between Failures
- Is the time between failures of a device
- Is used as a hardware availability metrics
- Is about the quality and reliability of an asset
- $MTFB = \text{Total Operational time} / \text{total break downs}$

Example:

Total operational time = 1000

Total break downs = 5

MTFB - 200



MTBF stands for Mean Time Between Failure. A device may have failed 100 days back and failed again at present times. If you calculate this without calculating its overall operational time, the MTBF is about 100 days. However, you need to calculate the MTBF with the total operational time of the device.

In the networking world, MTBF is used as a hardware availability metric. If you need to know the total availability of the device, then you need to use these metrics. Higher the MTBF, better the reliability, quality, and availability of the device.

Calculating the MTBF is quite easy. You can use the following formula:

$MTFB = \text{Total Operational time} / \text{total break downs}$

So, if the total operational time is 1000 hours and there have been a total of 5 break downs, you need to divide the total operational time, 1000, by 5, the total number of break downs. The answer you get is 200 hours, which is the MTBF.

# High Availability Measurements - MTTR

MTFB

MTTR

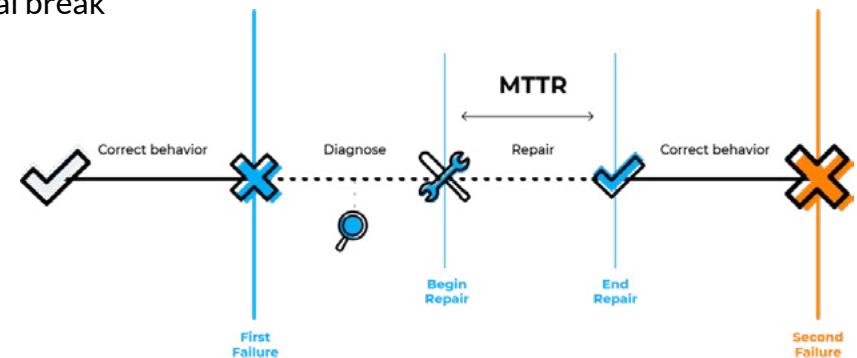
- Stands for Mean Time to Resolution
- Is the time taken to repair a failed device
- Includes the time from reporting the failure to getting the device up and running after repair
- $MTTR = \text{Total maintenance time} / \text{total break downs}$

Example:

Total maintenance time = 100

Total break downs = 5

MTTR - 20



MTTR stands for Mean Time to Repair. It is the time taken to repair a failed device. When a device fails, the failure of the device is reported to the concerned team. From reporting the failure to getting the device up and running, there is a time that is spent. This is the time that is known as the MTTS.

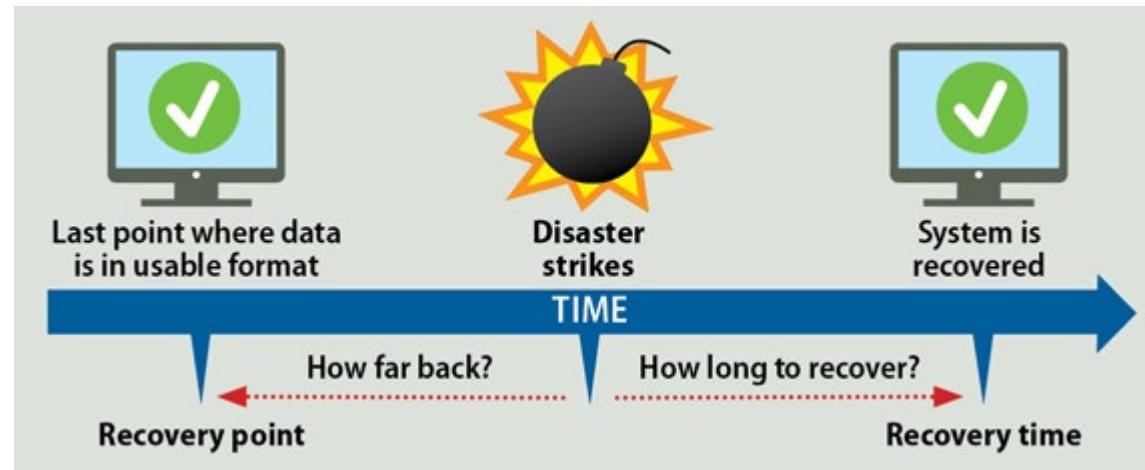
For example, if you had five breakdowns that took a total of 100 hours to repair the device. If you divide the 100 hours by 5, you get 20, which is the MTTR.

# Recovery Objectives - RPO

RTO

RPO

- Stands for Recovery Point Objective
- Defines how much data can be lost after a disaster
- Is the tolerance threshold for an organization



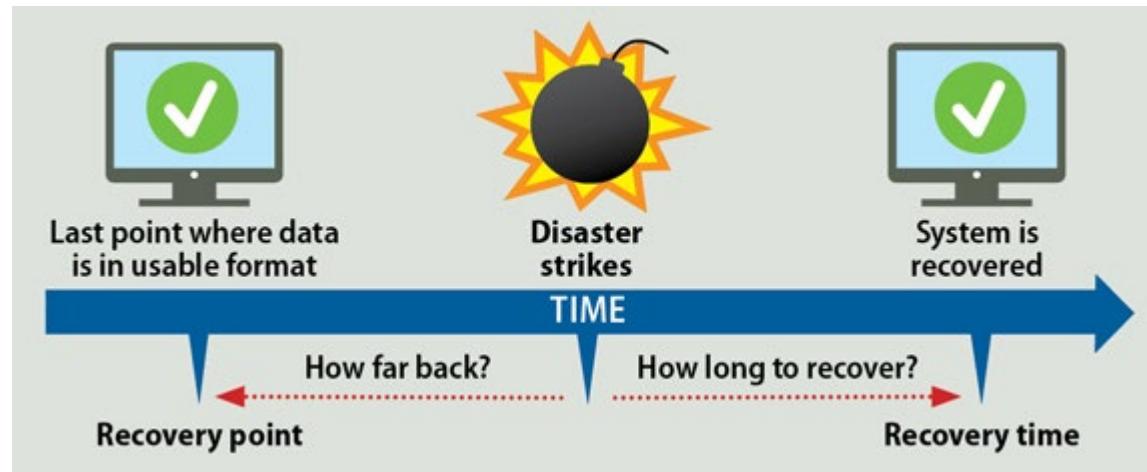
RPO stands for Recovery Point Objective, and it defines the amount of data that can be lost after a disaster. In the Business Continuity Plan (BCP), you usually have the RPO defined, clearly stating you can lose certain hours of data. For example, if your RPO is defined as 10 hours and your last backup is from 6 hours back, you are still within the range of the RPO.

# Recovery Objectives - RTO

RTO

RPO

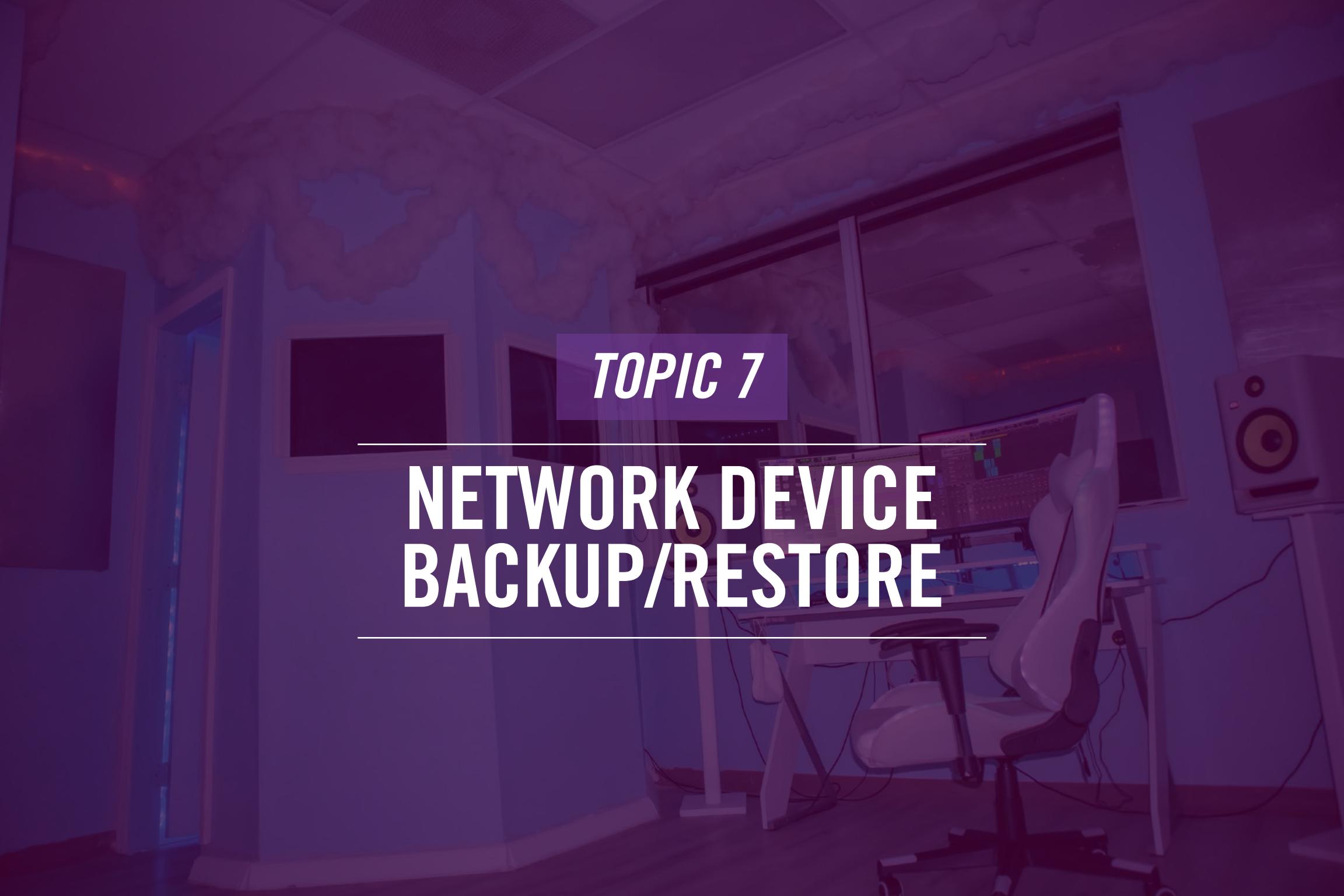
- Stands for Recovery Time Objective
- Is the amount of time an organization can afford the downtime
- Is the time in which the impacted services must be restored



RTO stands for Recovery Time Objective, which defines the time the business operations must be restored after a disaster. If this time exceeds, then there are unfavorable outcomes, like loss of data or even loss of business due to downtime.

In simplest words, it is the downtime that an organization can afford without impacting the unfavorable incident that caused the downtime. You can define RTO as the time of recovery since the incident was reported.

For example, if the RTO is one hour, a business can tolerate downtime. Beyond this time, there are unfavorable outcomes like loss of business.



## *TOPIC 7*

---

# NETWORK DEVICE BACKUP/RESTORE

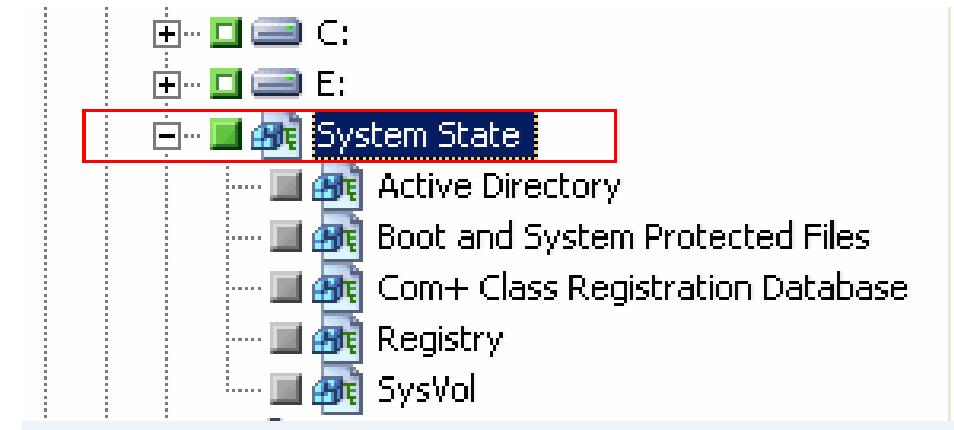
---

# Network Device Backup/Restore – State

Configuration

State

- Contains operating system components, configuration files, boot files, registry and COM+ database
- Is usually performed when making a change to an operating system
- Is used to revert if the operating system crashes



A state backup is also known as the system state backup. It is performed to back up the operating system, its files, register, and the COM+ database – things required to make a system functional.

In the Windows environment, you can perform a system state backup when making changes to the system. In case of a failure, you can restore the system from the system state backup. When you perform the restore, the system reverts to the time when you had taken the backup. You can then revert to the system state backup, and the newly updated device drivers will not be available anymore. Let's simplify this a little more. You performed the system state backup. After the backup, you updated the device drivers, and the operating system became unstable. This is because you had performed the system state backup before installing the drivers.

An important point to note is that the system state does not back up the data. They are usually smaller in size and are quick to restore. You must perform a data backup, something like a full backup, which can be coupled with incremental or differential backup.

# Network Device Backup/Restore – State

Configuration

State

- Backs up the configuration of an existing system that can be used to restore the system
- Should be encrypted when backed up to avoid misuse
- Can be done:
  - Manually
  - Using an automation application that backs up the configuration after detecting changes
  - Scheduled

Several networking devices, like routers and switches, do not have the provision of system state backup. They have the configuration that needs to be backed up. You perform the configuration backups with these devices by backing up the configuration files, which are later required to restore the device.

When you back up the configuration files, you should store them safely. This is because hackers look for such files that can give them insights into devices configuration and makes their lives easier when breaking into these devices. Therefore, all configuration files that you backup should be encrypted.

Configuration backups can be performed manually. However, there are several automation applications available that help you back up the configuration of network devices. Some devices also provide the provision for a scheduled backup.



# Summary

- Load balancing
- Multipathing
- Network interface card (NIC) teaming
- Redundant hardware/clusters
- Facilities and infrastructure support
- Redundancy and high availability (HA) concepts
- Redundancy and high availability (HA) concepts



That's the end of the lesson.

Here we covered:

- |  |   |
|--|---|
| <ul style="list-style-type: none"><li>• Load balancing</li><li>• Multipathing</li><li>• Network interface card (NIC) teaming</li><li>• Redundant hardware/clusters</li></ul> | <ul style="list-style-type: none"><li>• Facilities and infrastructure support</li><li>• Redundancy and high availability (HA) concepts</li><li>• Redundancy and high availability (HA) concepts</li></ul> |
|--|---|



*NEXT TOPIC*

---

# COMMON SECURITY CONCEPTS

---

---

# MODULE 4

---

# Module 4

LESSON 1 EXPLAIN COMMON SECURITY CONCEPTS

LESSON 2 TYPES OF ATTACKS

LESSON 3 NETWORK HARDENING TECHNIQUES

LESSON 4 REMOTE ACCESS METHODS

LESSON 5 PHYSICAL SECURITY



Lesson

1

---

# Explain Common Security Concepts

- 1 — Welcome to the first lesson of Module 4. In this lesson, you will learn about the:
  - 2 — Explain Common Security Concepts
- 



Network Fundamentals

# Agenda

- CIA Triad
- Threats
- Vulnerabilities
- Exploits
- Least privilege
- Role-based access
- Zero Trust
- Defense in depth
- Authentication methods
- Risk Management
- Security information and event management (SIEM)



Hi, welcome to COMPTIA Network+ Course

In this lesson, we will talk about:

- CIA Triad
- Threats
- Vulnerabilities
- Exploits
- Least privilege
- Role-based access
- Zero Trust
- Defense in depth
- Authentication methods
- Risk Management
- Security information and event management (SIEM)





**TOPIC 1**

---

**CIA TRIAD**

---

# CIA Triad

- Is the core principle of cybersecurity
- Defines Confidentiality, Integrity, and Availability
  - Confidentiality: Prevents unauthorized access to data
  - Integrity: Prevents unauthorized modification of data
  - Availability: Ensures availability of information as and when required



Everything is information security or rather any form of security is based on the CIA triad, which has three key components:

- Confidentiality: This is about protecting the information from any unauthorized access.
- Integrity: Is about preventing any types of unauthorized modifications or alteration of the data
- Availability: Ensuring the information is available as and when required to the authorized individuals

These are just the basic definitions. In the coming slides, you will learn about these concepts in more detail.

# Confidentiality

Availability

Integrity

Confidentiality

- Can be jeopardized by various methods, such as:
  - Network traffic capture
  - Stealing passwords
  - Social engineering
  - Shoulder surfing
- Can be protected by various methods, such as:
  - Encryption
  - Access control
  - Data classification
  - Personnel training
- Has various relevant concepts, such as concealment, secrecy, and privacy



# Confidentiality

Now, in the previous slide, you learned the basic definition of confidentiality. It is the first pillar or principle of the CIA triad. When you refer to confidentiality, you want to ensure that the information is protected and cannot be accessed by unauthorized individuals. For example, in movies, you would have seen a file that has confidential written it. This means that the file is to be opened only by one or more authorized individuals. If anyone else opens the file, then confidentiality is breached.

In the digital world, confidentiality is breached by various methods. It could be network traffic capture to find user credentials. It could also be stealing passwords or performing social engineering. For example, an attacker may send out a phishing email with a malicious link. This is social engineering. When users fall for the trick, they may click on the malicious link, which drops malware onto their system. The malware may capture the keystrokes or send out information to the attacker.

Shoulder surfing is another method that insider performs. For example, while the human resources representative is entering some confidential data about the employees, another employee comes and stands behind him. The employee can read through the confidential data. This is shoulder surfing.

Now, you can protect confidentiality using various methods. It is important to note that not all methods can be applied in every situation. You may have to select the appropriate method.

- Encryption – applied to data at rest and data in motion
- Access control – grant appropriate permissions to the authorized individuals
- Data classification – define the different categories of data – classified, private, public, etc.
- Personnel training – Required to prevent users from falling as prey to the attackers

Confidentiality has various relevant concepts, such as:

- Concealment: Preventing access to the information
- Secrecy: Ensuring that the information is kept secret.
- Privacy: Protect the information that can be personal or confidential



# Integrity

Availability

Integrity

Confidentiality

- Is about maintaining consistency and accuracy of data
- Is about preventing:
  - Authorized individuals to make unauthorized changes
  - Unauthorized individuals to make any changes
- Can be verified by checksum
- Can be threatened by malware and coding errors
- Can be prevented by methods, such as access control, encryption, and data input validation
- Is relevant to accuracy, authenticity, and validity



# Integrity

The second important concept of the CIA Triad is integrity, which is about maintaining the accuracy and consistency of data. Let's say that you saved a file with some content. If someone has changed the contents of the file, then the integrity of the file is lost. This is because the data, as per you, is no longer accurate.

Integrity can be in danger because of unauthorized and authorized individuals. It can be the authorized individuals who make unauthorized changes. For example, if you were to edit only a specific section, you intentionally change the values in another section. On the other hand, it is unauthorized individuals making changes without permission.

Each file has a specific checksum. When a file is created, it has a checksum even if the file is blank. If you add data, the checksum changes. When you want to verify the integrity of a file, you need to know the original checksum and compare it. This is typically done when you download a file from the Internet. The file provider usually mentions the checksum of the file. After you download it, you can calculate the checksum and match it with the original checksum. If both checksums match, you know the file is as it should be.

So, other than the authorized users making unauthorized changes or making changes, other entities can cause harm to the integrity of a file. For example, malware and coding errors can also cause harm to the file's integrity. Malware can change the file by embedding its code, or a coding error can change the values in a database.

To prevent integrity, you can put various methods into practice. You can implement access control, encryption, and data input validation. For example, encryption protects the confidentiality and integrity of a file.

Integrity has various relevant concepts, such as:

- Accuracy
- Authenticity
- Validity

Each of these words is like a synonym to integrity.

# Availability

## Availability

## Integrity

## Confidentiality

- Is about making the information available as and when required
- Is also about providing uninterrupted access
- Can be threatened by:
  - Device failure
  - Natural or man-made threats
  - Code errors
- Can be protected by:
  - Monitoring devices and network
  - Redundancy
  - Backups
- Relates to various concepts such as business continuity, backups and restore

The third principle of the CIA Triad is availability. You need to have the data available as and when required. Even if you can maintain confidentiality and integrity, if the data is unavailable when required, it may be of no use later. Along with confidentiality and integrity, the data must be available to the authorized candidates as and when required. The authorized should have uninterrupted access to the information.

Just like confidentiality and integrity, availability can also be threatened by various things like device failure, natural or man-made threats, and code errors. For example, code errors can wipe out the entire database or delete critical entries, impacting data availability.

You can also use various methods to protect the availability of the data and applications on the network. You can perform continuous monitoring of the device and the network. You can configure redundancy of the data and applications to make them available around the clock. You can configure data to be backed up regularly.

The concept of availability also relates to business continuity and backup and restore.





## *TOPIC 2*

---

# THREATS

---

# Internal Threats

External

Internal

- Are internal to an organization
- Are difficult to detect in most cases
- Originate from users who know about the internal resources
- Are often the reasons for major incidents
- Some examples include:
  - Theft of devices
  - Unauthorized use of resources
  - Shadow IT
  - Unauthorized data sharing

As the name states, internal threats are internal to an organization. They are the employees or individuals who have links with an organization. For example, a vendor working with the organization and is stationed within the office can also be considered an internal threat.

The biggest risk about the internal threats is that they are difficult to detect. It is difficult to doubt your people – this is what the danger is all about. You can counter a threat if you know what it is. This is where the problem lies, as organizations often do not see their employees as a threat. Another reason is that the internal threats are inside the network – behind the firewall, so they don't get detected.

The internal users know a lot about the organization, its network, applications, and data. In totality, they know about the internal resources, which is the biggest risk for an organization. If one employee goes rogue, then the entire organization is at stake. Internal threats are often the reasons for major incidents. As per Verizon's reports, this number is around 22%, which is quite high. It is like several organizations are suffering from internal threats. However, it is always assumed that the internal threats are intentional, which is not the case. Several security incidents are caused by employees who are not security-aware or have caused an unintentional incident. For example, an employee deleted a set of confidential and critical files without knowing what they were. It is an incident that was not intentional.

Some of the key examples of internal threats are:

- Theft of devices: An employee walking away with a hard drive on the last day of his job
- Unauthorized use of resources: An employee downloading and installing pirated software
- Shadow IT: An employee setting up his webserver
- Unauthorized data sharing: An employee sending a confidential file to a friend outside the organization



# External Threats

External

Internal

- Generate from outside the network
- Exploit the system or application vulnerabilities
- Target the users in most cases
- Can be generated by different types of threat actors, such as:
  - Script kiddies
  - Advanced Persistent Threats (APTs)

In oppose to the internal threats, the external threats originate from outside the network. They are originated by external entities who want to exploit the system or application vulnerabilities. They have to get into the network to cause damage or steal data. In most cases, the users are the target of these attackers.

In the old days, the attackers targeted the servers, firewalls, and edge routers. However, the trends have changed. The users are now being targeted as they are considered to be a soft target. Once the targeted user makes a mistake, the attackers find an easy way to get into the network. For example, a user falls for a phishing email and clicks on the malicious link within the email. Malware is downloaded on the user's system, and that is all it takes for the attacker to exploit the vulnerabilities within the systems and applications.

An attacker is the threat actor who wants to damage the systems and data or gain control of them. There can be different threat actors like script kiddies, who rely on other people's tools, or the Advanced Persistent Threats (APTs) who develop their sophisticated tools.



> Access Granted

## TOPIC 3

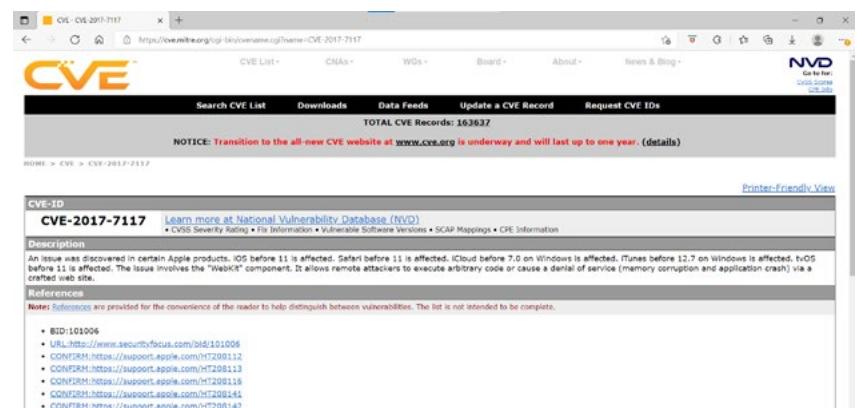
# VULNERABILITIES

# Common Vulnerabilities and Exposures (CVE)

## Zero Day

## Common Vulnerabilities and Exposures (CVE)

- Is a list of commonly known vulnerabilities and system flaws
- Has a CVE ID, such as CVE-2017-7117
- Is maintained by MITRE.org
- Has information about the vulnerability and may also contain the solution



Common Vulnerabilities and Exposures (CVEs) is a database that has a list of already identified vulnerabilities. It is a consolidated database that serves as a repository for anyone to come and locate a particular vulnerability's details.

The vulnerabilities are identified by a vulnerability number known as CVE ID, such as CVE-2017-7117. The first set of four numbers, such as 2017, is when the vulnerability was identified.

The CVEs database is owned and maintained by the MITRE Corporation. In the database, you can search the vulnerability based on an application name or the CVE ID. Each vulnerability is explained thoroughly – the nature of the vulnerability, its description, number, and the solution to mitigate the vulnerability.

# Zero-day

## Zero Day

## Common Vulnerabilities and Exposures (CVE)

- Is a vulnerability that can be exploited and is not known to the product company
- Has no patch or security update as it is still unknown
- Is exploited by the attackers
- Can exist in:
  - Operating systems
  - Web browsers
  - firmware
  - Internet of Things (IoT)
  - Applications
  - Hardware

The vulnerabilities that have been located and discovered will have a solution to patch them up. However, the vulnerabilities that are not located can always be exploited. Let's assume that you are using an application that you purchased from a vendor. You test the application and find a vulnerability that has never been discovered before. This is a zero-day vulnerability. Because it has been recently discovered, it is obvious that there is no fix or patch for this vulnerability.

Attackers or security researchers can discover zero-day vulnerabilities. Attackers find such vulnerabilities to exploit them. Such vulnerabilities help them get inside a network or exploit applications to steal data from the backends. Attackers take advantage of these vulnerabilities, and security researchers usually inform the vendor about the vulnerabilities to be patched immediately.

Zero-day vulnerabilities can exist in almost every type of application and hardware. It can exist in applications, operating systems, web browsers, IoT, and the hardware or its firmware.

## *TOPIC 4*

---

# EXPLOITS

---

# Exploits

- Is a code that takes advantage of a security flaw or vulnerability
- Can be client-side or server-side
- Allows the attacker to perform several tasks, such as:
  - Remotely control the systems
  - Perform privilege escalation
  - Exfiltrate data



An exploit is a piece of code that is designed to take advantage of a specific vulnerability. Networks are usually protected with several security hardware or applications. It can be difficult for an attacker to get into a network. However, if an attacker finds a vulnerability, it can take advantage of it using an exploit, which can be readily available in applications like Metasploit or custom developed.

The exploits can be either client-side or server-side. The client-side exploits are focused on exploiting the vulnerabilities in client-based applications like a Web browser. These exploits can be focused on exposed services on a client system, clients exposed to a malicious server, or social engineering attacks to install malicious applications.

On the other hand, the server-side exploits focus on attacking the servers. It can be the operating system, applications, or services on the server. With the server-side exploits, the main intent is to gain credentials and then perform the lateral movement on the network.

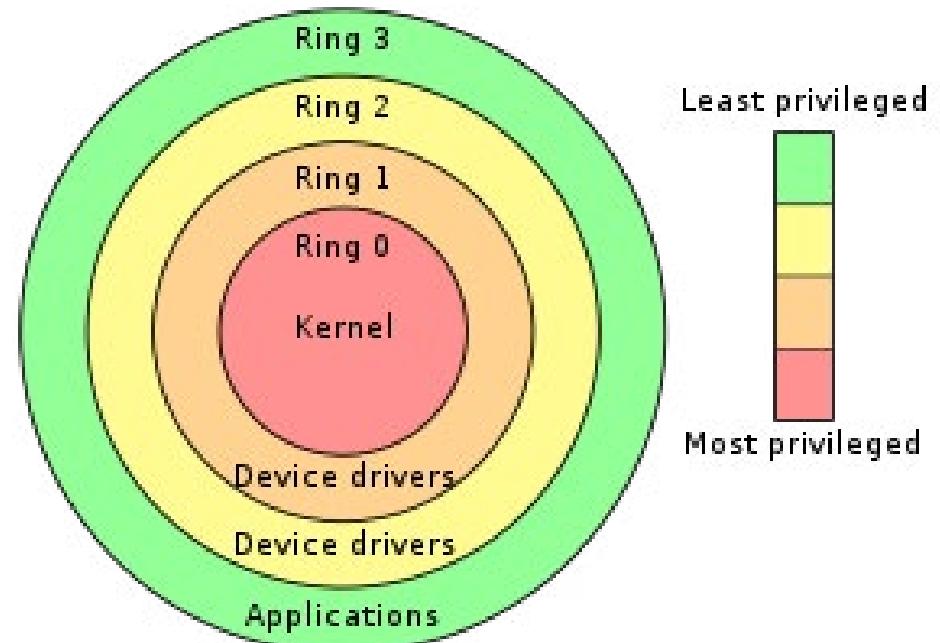
An attacker can use the exploits in different ways. It could be to remotely control the system, perform privilege escalation, specifically with the server-side exploits, and exfiltrate data from the systems.

## *TOPIC 5*

# LEAST PRIVILEGES

# Least Privileges

- Allows the administrators to grant only the permissions to the users that are required for them to perform their jobs
- Does not allow extra permissions to be granted
- Is similar to the need-to-know principle
- Enforces minimum access to the users



[Principle of least privilege - Wikipedia](#)

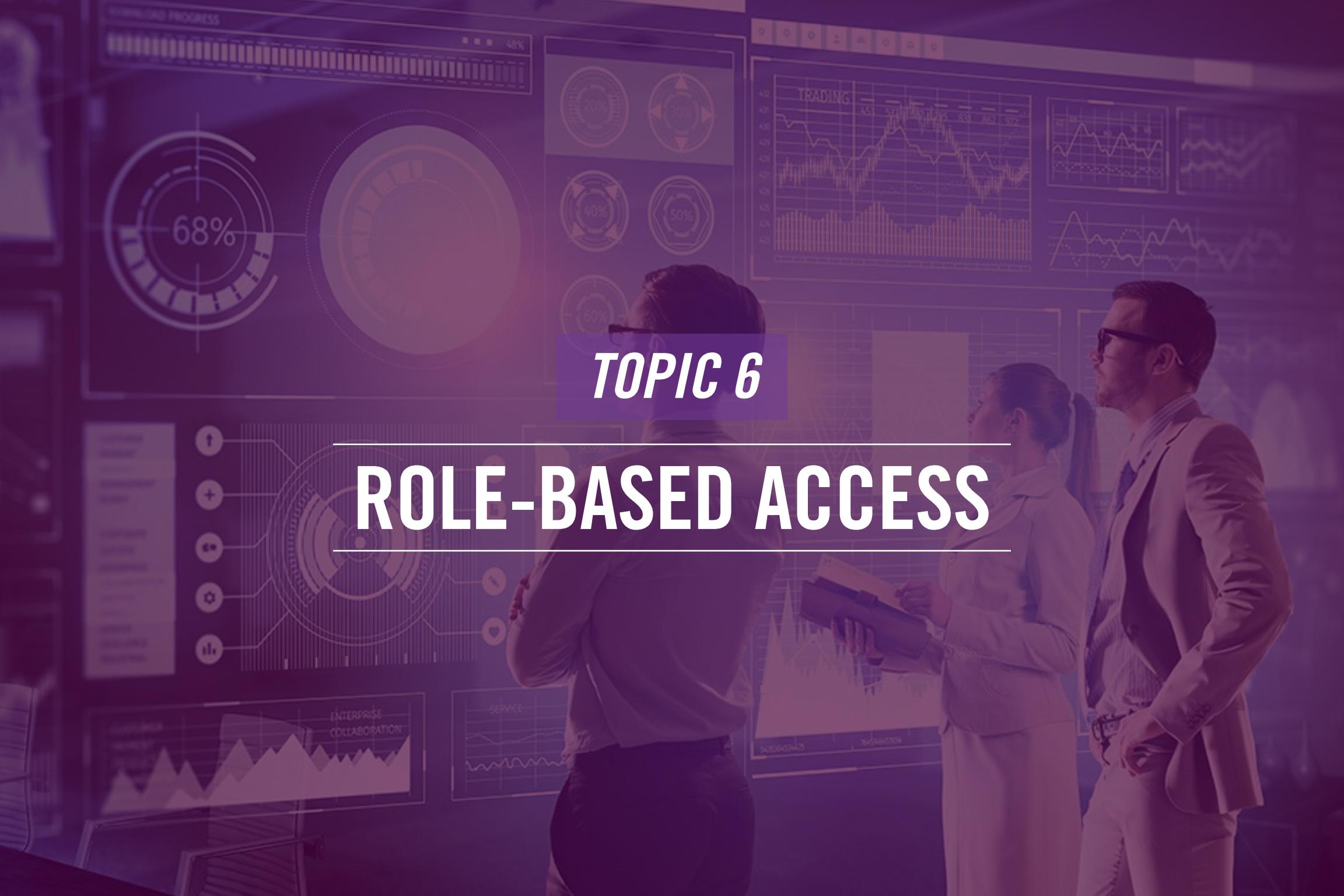
The principle of least privileges allows the administrators to grant only the permissions to the users required to perform their jobs. For example, if a user is only required to validate the data but not alter it, do not write permissions. The user should be granted only read-only permission.

The users with extra privileges tend, intentionally or unintentionally, to alter the data, which is not required to be done. To prevent this, the principle of least privileges comes in handy. Several administrators allow the users to have full control of their systems. Users tend to download applications, and sometimes, they may even download pirated applications to perform a task.

The principle of least privileges works similar to the need-to-know principle – you should only know what you need to know. Nothing more or nothing less. This is what the principle of least privileges is stating in the context of the privileges or permissions. You will get only the permissions that are required for you to work. With this principle, minimum privileges are granted to the users.

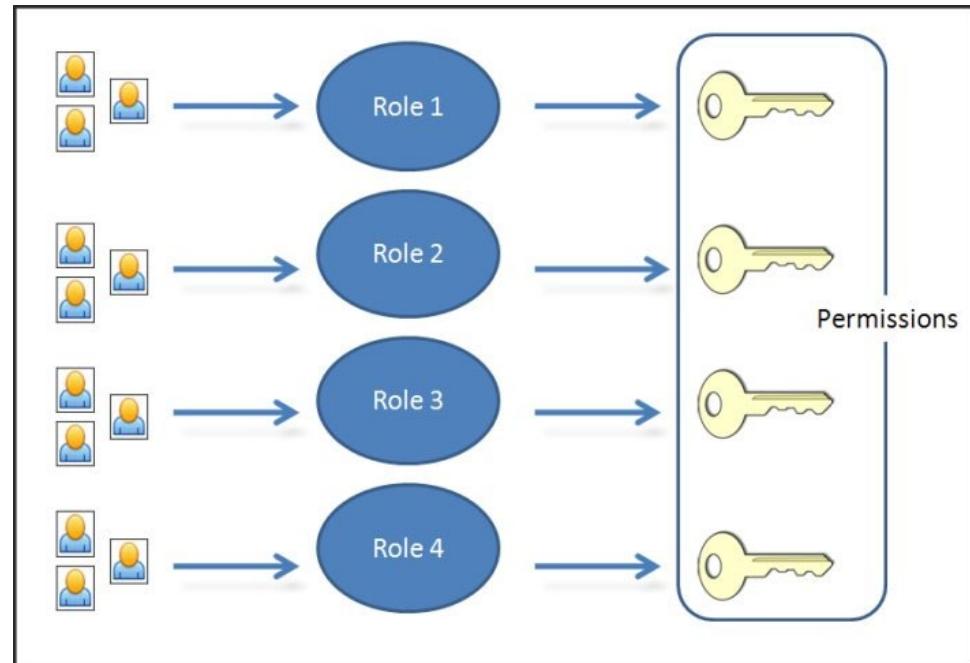
## *TOPIC 6*

# ROLE-BASED ACCESS



# Role-based Access

- Is the access granted to a group of users based on their roles
- Has specific permissions assigned to the group
- Uses the principle of least privileges
- Assigns the permissions necessary to do their jobs



Several users in an organization may need similar kinds of privileges. Let's assume that you have a database application. Five users are validating the data within the database. You can either assign them permissions individually or create a group, such as database validators, and add these users to this group. This is a role that you have created and assigned permissions to it. It is also easy to manage a group rather than individual users. You can add or remove users from the group while it has the permissions on the database or an application.

With role-based access, you work with the principle of least privileges. You need to assign minimum privileges to the role that should be sufficient to perform their job function. Extending the database validators group, you do not need to assign them the database write permissions. The read permission on the database is sufficient.



*TOPIC 7*

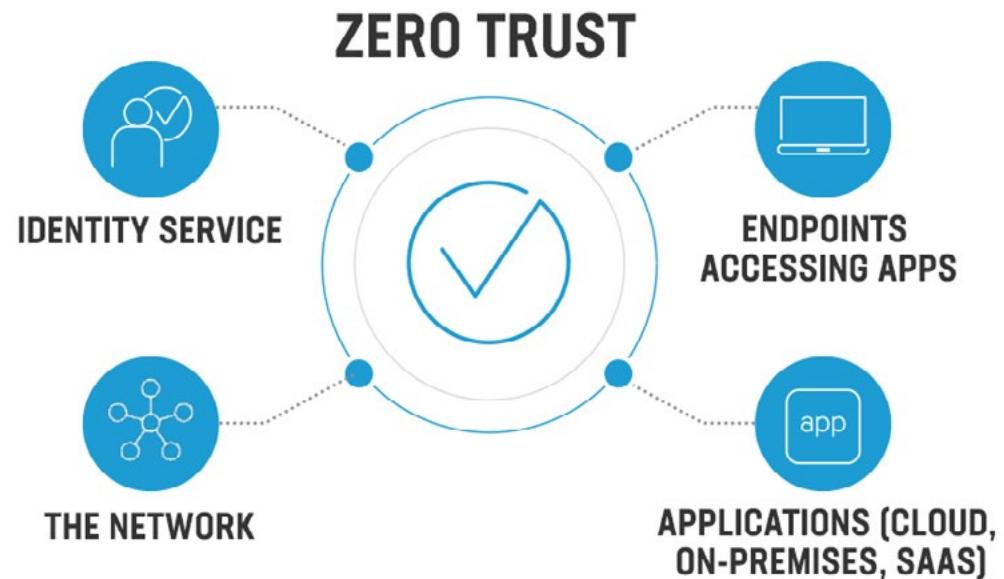
---

# ZERO TRUST

---

# Zero Trust

- Is a security architecture that requires every user to be authenticated before granting access
- Uses the “never trust, always verify” concept
- Is designed to eliminate trust by default
- Is applied to internal as well as external users



Sometimes, it is fine not to trust anyone – this is what the zero-trust concept is based on. This concept is relatively new that is being adopted by organizations. The concept states that every user connecting to the network should be authenticated and authorized to access the required resources. By default, no one should be trusted. It works with the concept of “never trust, always verify.” It is like the security guard at the main gate of your office knows you well, but he requires you to show the identity card daily.

The concept of zero-trust eliminates the concept of trust on which the networks were earlier based, but they are not shifting towards the zero-trust concept. In zero-trust, every user, whether internal or external, needs to be authenticated.

It is critical to understand that the organizations are now geographically spread, and therefore, the data and users are also in different locations. You cannot enforce zero-trust in one location, let's say the headquarters. It has to be enforced on all locations covering the entire network.



*TOPIC 8*

---

# DEFENSE IN DEPTH

---

# Defense-in-Depth – Network Segmentation

## Honeypot

- Is used for security and ease of administration
- Is used to control the flow of information
- Can be performed at several layers of the OSI model
  - Layer 1 – Physical segmentation
  - Layer 2 – VLANs on switches
  - Layer 3 – Access control lists on routers

## Network Access Control

## Separation of Duties

## Screen Subnet

## Network Segmentation Enforcement

Large networks are difficult to maintain from the ease of administration and security. You can break a large network into segments and control the flow of information. A large, flat network is an ideal target for attackers. You get in once, and then everything is there in front of you. To ease out this situation, you can segment the network to limit the attack surface. The flow of information can be controlled between the segments, which eventually can restrict the attacker if one segment has been attacked. It also limits the network congestion in a segment.

The segmentation can be performed at several layers of the OSI model. For example:

- Layer 1 – Physical segmentation. This requires physical separation of the network.
- Layer 2 – VLANs on switches. This requires VLAN implementation on switches.
- Layer 3 – Access control lists on routers. This requires using access control lists on routers. You can limit the access of one segment to another.



# Defense-in-Depth – Screen Subnet

Honeypot

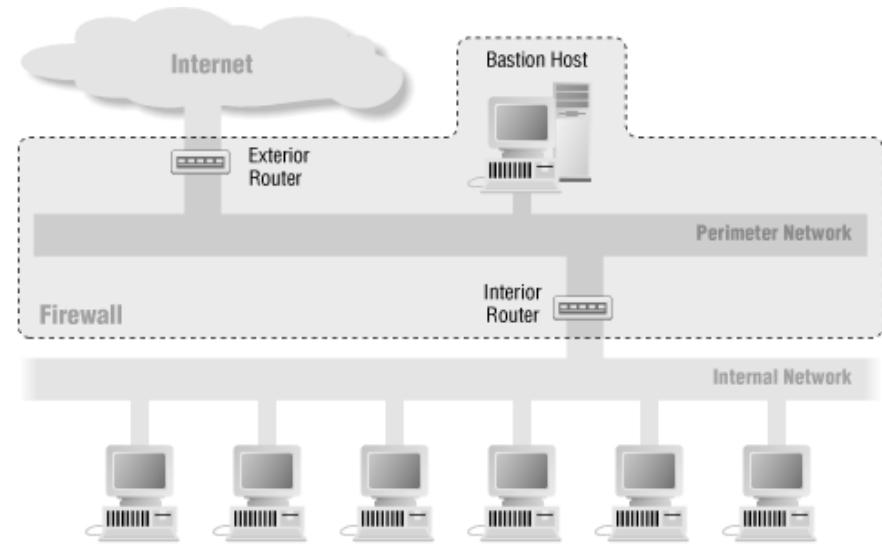
Network Access Control

Separation of Duties

**Screen Subnet**

Network Segmentation Enforcement

- Is also known as Demilitarized Zone (DMZ)
- Contains the servers that need to communicate on the Internet
- Is mainly used to protect the internal systems
- Is a subnet that is separated by:
  - An outer or perimeter router facing the Internet
  - An internal router separating it from the internal network



Screen subnet is also known as demilitarized zone or DMZ. In an organization, there can be several Internet-facing servers. If they are on the same network segment as the rest of the system, they can pose a great risk for the entire network. If any of these servers get compromised, the attacker will get to the remaining systems without any problems. You put the Internet-facing servers into a separate segment to solve this problem, limiting the traffic to the internal network. In such a scenario, if there is an attack on the DMZ servers, the internal network is protected as it is separated.

In the DMZ, you can place servers that need to communicate on the Internet. Some of these servers can be web, FTP, and messaging servers.

The DMZ works with two routers. The first router is the access router that separates the Internet from the DMZ. The second router is the choke router that separates the DMZ from the internal network.

# Defense-in-Depth – Separation of Duties

Honeypot

- Divides a task into two parts and assigns each part to an individual
- Requires both to complete their parts to complete the task
- Is used to prevent any fraud or wrongdoing by an individual who solely owns the task
- Has been used for several decades – leave and reimbursement authorization by a manager and head of the department

Network Access Control

Separation of Duties

Screen Subnet

Network Segmentation Enforcement

The separation of duties breaks down a task into two parts that are assigned to individuals. For example, if you have ever submitted a reimbursement voucher to your manager, it needs to be signed by the manager and the head of the department. If both the entities do not complete the approval process, then the task is not complete, which means you do not get the reimbursement.

The core intent of using separation of duties is to ensure that there is no fraud being committed. If one individual is approving the vouchers, then there can be chances that fraud can be committed. However, there are fewer chances that both individuals are involved in the fraud even though there is no surety on this but chances of it happening to reduce drastically.

Separation of duties is not a new practice. It has been in practice for a long time, specifically in accounts and finance.



# Defense-in-Depth – Network Access Control

## Honeypot

- Scans a system before it joins a network
- Can also remediate the device if the system's state does not meet the requirements
- Ensures that no unsafe system connects to the network
- Has the capabilities of:
  - Policy management
  - Guest networking
  - Security posture check
  - Incident response

## Network Access Control

## Separation of Duties

## Screen Subnet

## Network Segmentation Enforcement

The next part of Defense-in-Depth is NAC or Network Access Control, preventing unsecured or vulnerable systems from connecting to a network. Without a NAC, a system can connect to a network without any problems. A vulnerable system connecting to a network can impose greater risks to the network. However, when you implement a NAC, it scans the system before it joins a network. It checks the system for compliance, such as antivirus and operating system updates. If everything is found to be compliant, then the system is granted access to the network resources.

If the system does not meet the compliance requirements, the NAC can be configured to remediate the non-compliant systems. Once they are compliant, the systems are allowed to connect to the network.

With NAC in place, it ensures that no unsecured system connects and poses threats to the network.

A NAC has several capabilities, such as:

- Policy management: can pose different policies for different operating systems
- Guest networking: includes a guest self-service portal that can help them with several tasks, such as guest registration
- Security posture check: Can check the compliance on systems
- Incidence response: Can block, allow, or remediate systems without any human intervention



# Defense-in-Depth – Honeypot

## Honeypot

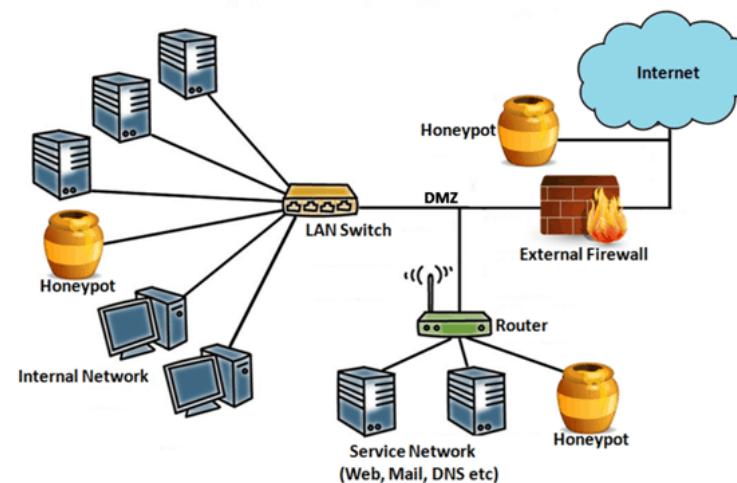
- Is used to lure hackers to understand their methods and tactics
- Runs applications and services and contains “real-look-alike” data
- Has reasonable security to look like a real system
- Is used as a diversion point

## Network Access Control

## Separation of Duties

## Screen Subnet

## Network Segmentation Enforcement



In simplest words, a honeypot is a trap that is set up for hackers. It is designed to lure hackers with a few applications and real-look-alike data. There is some level of security implemented to fool the attacker. Think of it like this – you find a server on the Internet that has no security and a bunch of data on it. It is too unrealistic. This would immediately alert the attacker that this could be a trap. Therefore, almost a real-look-alike system is simulated.

A honeypot is also used as a diversion point for the attacker. When the attacker finds a honeypot, they do not know it is a trap or a honeypot unless you make it obvious. Rather than attacking the real network, there is a high probability that the attacker is diverted to the honeypot. Another key intent of a honeypot is that when an attacker attacks it, you want to study their actions and the methodology they follow. It can give you great insights into how the attacker is planning to attack the network. One of the important things to note about a honeypot is that there should be no activity on this server. If there is any activity, it should be the attacker who is in the system.



*TOPIC 9*

---

# AUTHENTICATION METHODS

---

# Authentication Methods - Multifactor

EAP

802.1X

Local  
Authentication

Kerberos

LDAP

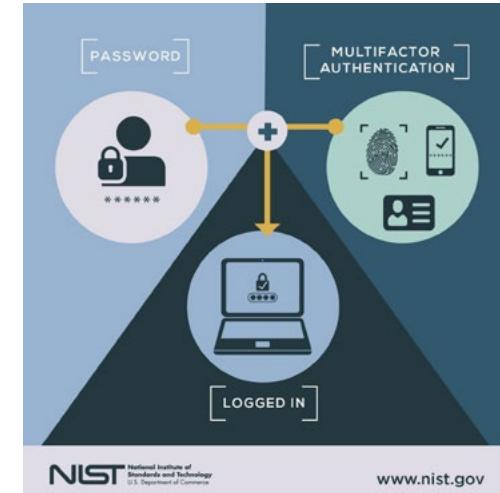
RADIUS

- Single sign-on  
(SSO)

TACACS+

Multifactor

- Is using more than two authentication factors
  - Using two factors method is two-factor authentication
- Can consists of:
  - Something you know – password
  - Something you are – physical trait, such as fingerprint
  - Something you have – smart card
  - Somewhere you are – geographic location
  - Something you do - behavior



On a network, most users are authenticated using their credentials, consisting of a username and password. However, passwords are prone to several attacks, such as brute-force and dictionary attacks. If a user's password is cracked, then the user can lose the account, which can further be misused, and therefore, passwords alone cannot be a method to protect the user's accounts.

To resolve the password issue, you can implement multi-factor authentication, which requires more than two authentication factors. You can use factors like:

- Something you know, such as password or PIN
- Something you are, such as retina, fingerprint, or facial recognition
- Something you possess, such as a smart card
- Somewhere you are, such as a location
- Something you do, such as your behavior

There is always confusion between two-factor and multi-factor authentication. Two-factor authentication uses two factors, such as a password and smart card. Multi-factor is using more than two factors, such as password, smart card, and location.

# Authentication Methods – TACACS+

EAP

802.1X

Local  
Authentication

Kerberos

LDAP

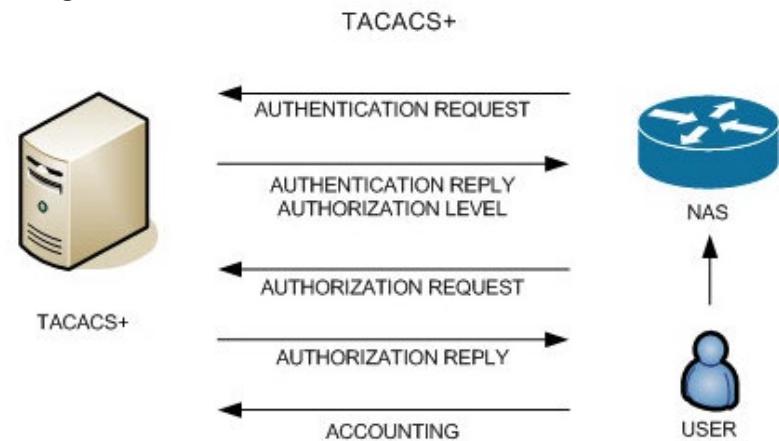
RADIUS

- Single sign-on  
(SSO)

TACACS+

Multifactor

- Performs authentication, authorization, and accounting
- Works with 802.1x capable devices, such as:
  - Switches
  - Wireless access points
- Uses TCP as the transport protocol
- Encrypts the entire packet



The Terminal Access Controller Access-Control System Plus (TACACS+) protocol uses the AAA method, including authentication, authorization, and accounting. It can work with devices that have 802.1x capabilities. For example, it could be a switch, wireless access point, or Remote Access Servers (RAS). An important thing to note is that authentication and authorization are kept separate.

Let's take an example of a user connecting to a RAS server. A connection request is sent to the RAS server, which forwards it to the TACACS+ system, reverts to the response. Then the RAS server sends the authorization request to the TACACS+ system, which then reverts with the authorization reply. When the user closes the session, the session is then accounted for and logged. TACACS+ performs the accounting based on:

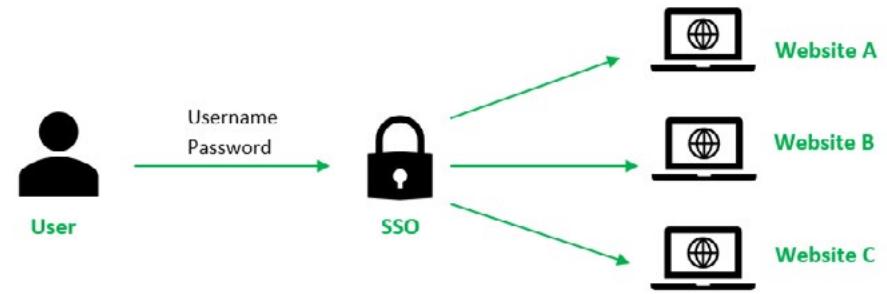
- Start and end time for the session
- Number of bytes sent and received during the session

TACACS+ uses TCP as the transport protocol and encrypts the entire packet.

# Authentication Methods – Single Sign-on



- Allows a user to access several network resources after authentication in a domain
- Is performed by assigning an access token to the user
  - Contains list of resources to which user has access
  - Use of token is transparent to the user



Organizations usually have a domain and several applications running. Think of a scenario where you have to log on to 10 different applications daily. This means that you have to remember 10 usernames and passwords. It is quite cumbersome to remember so many passwords. You can use one username and password to log on to all 10 applications with a single sign-on. A user logs on to the domain, and then access to the applications is granted by default.

The access is granted using an access token to the user. The access token contains a list of resources to which the user has access. When a user attempts to access a network resource, the access token is verified, and if the network resource is on the list, the user is granted access automatically.

The overall process of the access token is transparent to the user and happens in the background.

# Authentication Methods - RADIUS

EAP

802.1X

Local  
Authentication

Kerberos

LDAP

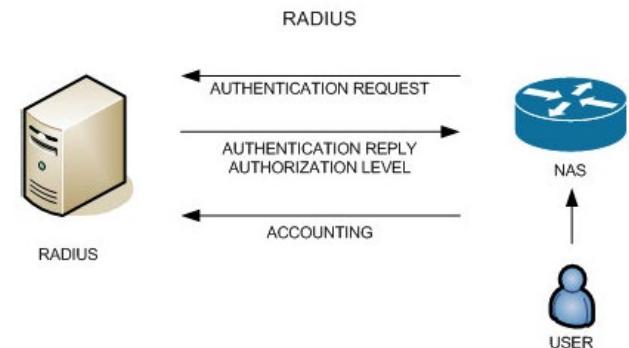
RADIUS

- Single sign-on  
(SSO)

TACACS+

Multifactor

- Is a client/server-based authentication and accounting service
  - Authorization is combined with authentication
  - TACACS+ keeps authorization separate
- Maintains the user profiles in a central database
- Performs the password encryption
- Uses UDP as the transport protocol
- Can be used with wired and wireless networks



RADIUS stands for Remote Authentication Dial-In User Service. It is a client/server-based authentication and accounting service. RADIUS and TACACS+ work similarly, but RADIUS combines authentication and authorization. TACACS+ keeps both of them separate. In RADIUS, there is no separate authorization request. It is only the authentication request, which includes the authorization request as well.

RADIUS uses a centralized database to authenticate users. For example, several Internet Service Providers (ISPs) use RADIUS and authenticate users when their requests are received for a connection.

Another fundamental difference with TACACS+ is that RADIUS only encrypts the password. On the other hand, TACACS+ encrypts the entire packet. Also, RADIUS uses UDP as the transport protocol. RADIUS can be implemented with wired and wireless networks.

# Authentication Methods – Single Sign-on

EAP

802.1X

Local Authentication

Kerberos

LDAP

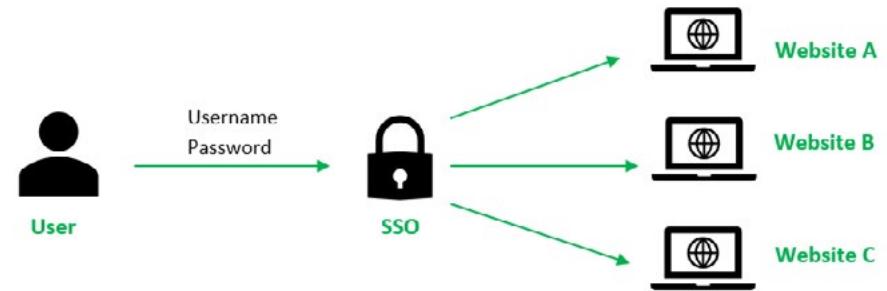
RADIUS

- Single sign-on (SSO)

TACACS+

Multifactor

- Allows a user to access several network resources after authentication in a domain
- Is performed by assigning an access token to the user
  - Contains list of resources to which user has access
  - Use of token is transparent to the user



Organizations usually have a domain and several applications running. Think of a scenario where you have to log on to 10 different applications daily. This means that you have to remember 10 usernames and passwords. It is quite cumbersome to remember so many passwords. You can use one username and password to log on to all 10 applications with a single sign-on. A user logs on to the domain, and then access to the applications is granted by default.

The access is granted using an access token to the user. The access token contains a list of resources to which the user has access. When a user attempts to access a network resource, the access token is verified, and if the network resource is on the list, the user is granted access automatically.

The overall process of the access token is transparent to the user and happens in the background.

# Authentication Methods - RADIUS

EAP

802.1X

Local  
Authentication

Kerberos

LDAP

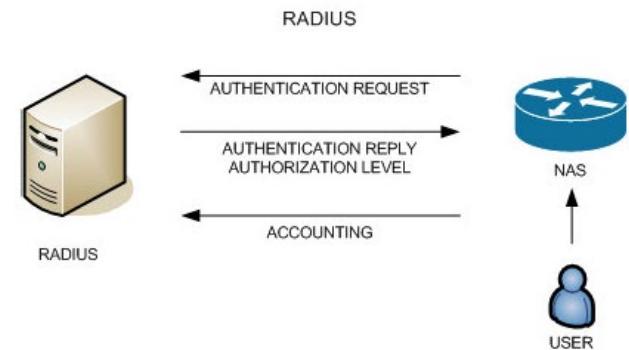
RADIUS

- Single sign-on  
(SSO)

TACACS+

Multifactor

- Is a client/server-based authentication and accounting service
  - Authorization is combined with authentication
  - TACACS+ keeps authorization separate
- Maintains the user profiles in a central database
- Performs the password encryption
- Uses UDP as the transport protocol
- Can be used with wired and wireless networks



RADIUS stands for Remote Authentication Dial-In User Service. It is a client/server-based authentication and accounting service. RADIUS and TACACS+ work similarly, but RADIUS combines authentication and authorization. TACACS+ keeps both of them separate. In RADIUS, there is no separate authorization request. It is only the authentication request, which includes the authorization request as well.

RADIUS uses a centralized database to authenticate users. For example, several Internet Service Providers (ISPs) use RADIUS and authenticate users when their requests are received for a connection.

Another fundamental difference with TACACS+ is that RADIUS only encrypts the password. On the other hand, TACACS+ encrypts the entire packet. Also, RADIUS uses UDP as the transport protocol. RADIUS can be implemented with wired and wireless networks.

# Authentication Methods - LDAP

EAP

802.1X

Local Authentication

Kerberos

LDAP

RADIUS

- Single sign-on (SSO)

TACACS+

Multifactor

- Is short for Lightweight Directory Access Protocol (LDAP)
- Maintains the data, such as usernames, passwords, email addresses
- Is queried by the applications for information on various resources
- Has several attributes, such as:
  - Common Name (CN)
  - Domain Component (DC)
  - Organizational Unit (OU)

LDAP stands for Lightweight Directory Access Protocol (LDAP). It is a directory service that maintains the data, such as usernames, passwords, and email addresses. It maintains a tree-like structure in which it stores the data for various resources, such as:

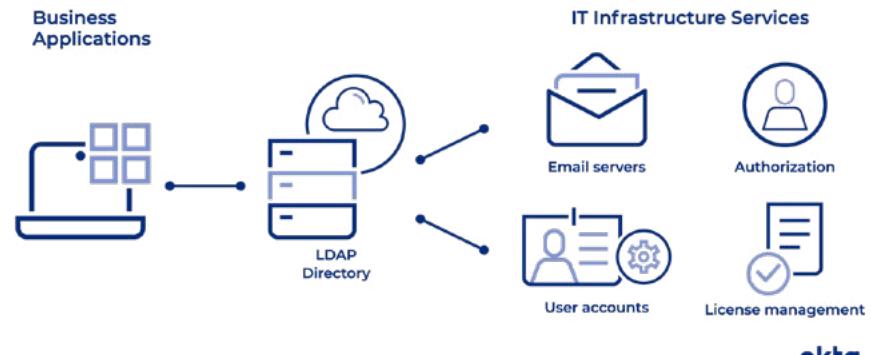
- Users
- Groups
- Systems

When an application needs to be equipped with authentication, it can work with local authentication, which means it will maintain its user database or integrate with LDAP services, such as Active Directory. Then, the application can use the LDAP database to authenticate users. The benefit of this is that the application does not need to store the user accounts and information. This task is then offloaded to the LDAP service.

LDAP has several attributes, such as:

- Common Name (CN)
- Domain Component (DC)
- Organizational Unit (OU)

## How LDAP Works



# Authentication Methods - RADIUS

EAP

802.1X

Local  
Authentication

Kerberos

LDAP

RADIUS

- Single sign-on  
(SSO)

TACACS+

Multifactor

- Is a security system that issues tickets to the users after they are logged in
  - With the tickets, users do not need to share the passwords
- Is used for providing authentication services over an insecure network
- Has three key components:
  - Client
  - Kerberos Key Distribution Center (KDC)
  - Server

Even though Kerberos is known to be a protocol, but that's an incomplete definition of it. Kerberos is more than just a protocol. It is a ticket-granting security system. When the users log on to the network, they are granted tickets, which are then used for communication over the network.

With the use of the tickets, which carry encrypted information, a user does not need to share the password for every communication on the network. The ticket takes care of the authentication part for the user. It is also important to note that tickets have a short validity period and expire when the validity period is over.

However, Kerberos refreshes the tickets for the users who are still logged on to the network. The refresh process remains transparent to the users.

There are three key components of Kerberos:

- Client: requests and receives the tickets from KDC
- Kerberos Key Distribution Center (KDC): issues the tickets to the clients
- Server: receives the tickets from the clients



# Authentication Methods—Local Authentication

EAP

802.1X

Local  
Authentication

Kerberos

LDAP

RADIUS

- Single sign-on  
(SSO)

TACACS+

Multifactor

- Uses the local user database for authentication
  - Verifies the username and password
- Uses Security Accounts Manager in Windows stored in C:\windows\system32\config\
- Uses the file named passwd in Linux stored in /etc/

User authentication can take place on the network through a centralized server or locally. Previously, you learned about LDAP that can be integrated with the applications for centralized authentication. The local authentication is performed on the system itself. It requires the user to provide a username and password. If you are a home user and are not connected to a network, then local authentication is performed every time you log on to the system. The username and password that you provide are authenticated locally.

Different operating systems store authentication information in different ways. In Windows, the information is stored in the Security Accounts Manager (SAM) database located in C:\windows\system32\config\. On the other hand, in Linux, all of its known distributions, the information is stored in the passwd file stored in the /etc/ directory.



# Authentication Methods – 802.1x

EAP

802.1X

Local Authentication

Kerberos

LDAP

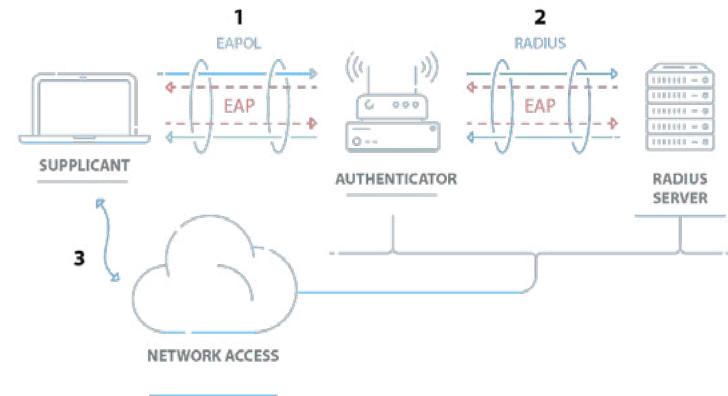
RADIUS

- Single sign-on (SSO)

TACACS+

Multifactor

- Is the centralized port-based authentication framework
- Works both on wired and wireless networks
- Has the following components:
  - Supplicant: client
  - Authenticator: Remote Access Servers, switches, wireless access points
  - Authentication server: RADIUS or TACACS+



The 802.1x method is a centralized authentication framework that works with wired and wireless networks. It is used for port authentication that requires the user to be authenticated. Once the user is authenticated, it authorizes the user and opens the ports for the user, who can be authenticated through the user credentials or a certificate.

There are three key components of 802.1x:

- Supplicant: a client who has requested to access the network
- Authenticator: Remote Access Servers, switches, wireless access points – these are the entities that received the request. It works like a postman. Once it receives the user credentials, it forwards them to the authentication server
- Authentication server: RADIUS or TACACS+ validates the received user credentials and sends a notification to the authenticator when the authentication is successful.

After the successful authentication, the supplicant or the client is allowed to access the required network resources.

# Authentication Methods - EAP

EAP

802.1X

Local  
Authentication

Kerberos

LDAP

RADIUS

- Single sign-on  
(SSO)

TACACS+

Multifactor

- Is used with the 802.1x framework
- Is used with wired and wireless networks
- Supports different authentication methods, such as:
  - One-time passwords (OTPs)
  - Smart cards
  - Public-key encryption authentication
  - Digital certificates
- Has variants, such as:
  - Protected Extensible Authentication Protocol (PEAP)
  - EAP-FAST
  - EAP Transport Layer Security (EAP-TLS)

EAP stands for Extensible Authentication Protocol (EAP). It is mainly used with the 802.1X port-based authentication framework that can be used with wired and wireless networks. Its main purpose is to authenticate clients.

EAP uses various authentication methods, such as:

- One-time passwords (OTPs)
- Smart cards
- Public-key encryption authentication
- Digital certificates

It also has variants, such as:

- Protected Extensible Authentication Protocol (PEAP)
- EAP-FAST
- EAP Transport Layer Security (EAP-TLS)

It is important to note that some of the variants use passwords, while others use certificates for which you need to have PKI or Public Key Infrastructure readily available.





**TOPIC 10**

---

**RISK MANAGEMENT**

---

# Risk Management

- Is an iterative process to minimize risks within an organization
- Focuses on:
  - Need to know what should be protected
  - Need to know how to protect the assets
  - Need to know if your approach is adequate
  - Need to monitor controls and improve them
- Has several phases:
  - Risk identification
  - Risk assessment
  - Risk control
  - Risk monitoring

As stated earlier, risks are inevitable, and they will happen. An organization should be well prepared in advance to either mitigate the risks or reduce their impact.

This is done through a well-defined risk management process, which is an iterative process that has several phases. You do not define the risk management process once and forget about it. It needs to be reviewed and iterated from time to time – risks will change from time to time. For example, you have discarded the old servers and moved the infrastructure to the cloud. The old risks are no longer valid, but the new risks related to the cloud environment are added.

With the risk management process, you:

- Need to know what should be protected – what are you trying to protect? Which assets are you protecting from risks? This is the risk identification step.
- Need to know how to protect the assets – When you have identified them, you need to know how you will protect them? This is the risk assessment step.
- Need to know if your approach is adequate – Are your approaches or methods of mitigating the risks are adequate? You need to use the appropriate controls to mitigate the risks. This is the risk control step.
- Need to monitor controls and improve them – Are you using continuous monitoring to mitigate risks? If a control fails to mitigate one or more risks, are you applying another control? This is the risk monitoring step.



# Security Risk Assessment—Threat Assessment

## Posture Assessment

- Is about identifying the threats and their related information through various sources

- Focus on the threats and their credibility
- Focus on their likelihood

## Penetration Testing

- Has a complete cycle:

- Initial assessment
- Review of the threat
- Plan to address the vulnerability
- Verify the credibility and likelihood of the threat

## Vulnerability Assessment

## Threat Assessment

Threat assessment is a method of identifying threats and their related information from various sources. You need to know the latest threats, their origins, and their impacts. You need to perform a threat assessment by getting as much information as possible to gain all this information. You need to know the following information:

- Threats
- Credibility
- Likelihood of occurrence

Organizations typically subscribe to the threat feeds that provide all this information to them. The threat feeds provide information about the latest threats that are emerging. The threat may provide information, such as:

- Suspicious domains
- Known malware hashes
- IP addresses that are known to roll out malware or linked with malicious activities

Threat assessment is a complete process that has several steps. It starts with the initial threat assessment. Then, you need to review the threat in question. If there is a vulnerability in the network relating to the threat, you need to perform the next step and plan to address the vulnerability. Finally, you need to use the R-S-I-F indicators, which stand for Recency-Severity-Intensity-Frequency. With the RSIF indicators, you can determine the likelihood and impact of the threat.

# Security Risk Assessment—Vulnerability Assess

## Posture Assessment

- Is the process of discovering and identifying the security weaknesses or vulnerabilities

## Penetration Testing

- Is an automated process performed with the help of a tool
- Can be of different types:

- System
- Application
- Network – wired and wireless
- Database

- Follows a complete cycle from identification to remediation

## Vulnerability Assessment

## Threat Assessment

Threat assessment is a method of identifying threats and their related information from various sources. You need to know the latest threats, their origins, and their impacts. You need to perform a threat assessment by getting as much information as possible to gain all this information. You need to know the following information:

- Threats
- Credibility
- Likelihood of occurrence

Organizations typically subscribe to the threat feeds that provide all this information to them. The threat feeds provide information about the latest threats that are emerging. The threat may provide information, such as:

- Suspicious domains
- Known malware hashes
- IP addresses that are known to roll out malware or linked with malicious activities

Threat assessment is a complete process that has several steps. It starts with the initial threat assessment. Then, you need to review the threat in question. If there is a vulnerability in the network relating to the threat, you need to perform the next step and plan to address the vulnerability. Finally, you need to use the R-S-I-F indicators, which stand for Recency-Severity-Intensity-Frequency. With the RSIF indicators, you can determine the likelihood and impact of the threat.



# Security Risk Assessment–Penetration Testing

## Posture Assessment

## Penetration Testing

## Vulnerability Assessment

## Threat Assessment

- Is an extension of vulnerability assessment
  - After identification, it exploits the vulnerabilities
  - Remediation is done at the end of the testing lifecycle
- Is a manual process of exploiting the vulnerabilities
- Is highly intrusive to simulate the real-life attacks
  - Highly focused with specific objectives
  - Simulates the possible paths taken by an attacker
- Has a specific goal for finding and exploiting the vulnerabilities
  - Vulnerability assessment – breadth over depth
  - Penetration testing – depth over breadth

Penetration testing is the next step of vulnerability assessment. In penetration testing, you identify the vulnerabilities and then exploit them. However, the intent of penetration testing is different from the vulnerability assessment. The penetration testing occurs after the vulnerability assessment, which helps you identify the vulnerabilities, and you perform remediation at the end of the vulnerability assessment. The remediation is done at the end of the penetration testing.

Unlike the vulnerability assessment, penetration testing is a manual process. After you identify the vulnerabilities, you need to exploit them manually. You can take one vulnerability at a time and start exploiting them. You want to see the damage that the vulnerability can cause.

Because penetration testing exploits the vulnerabilities, it is highly intrusive. It attempts to simulate the scenario of how an attacker would have exploited the vulnerability. This is necessary because you want to think like an attacker who would have exploited the vulnerability.

Penetration testing is about having a specific goal. For example, you can perform penetration testing of an application or the entire network. There is a specific objective behind it. Vulnerability assessment is broad – it attempts to find as many vulnerabilities as possible. On the other hand, penetration testing goes deep and exploits the vulnerabilities. It stops after finding the vulnerabilities and then you move into patching or mitigating the vulnerabilities.



# Security Risk Assessment – Posture Assess

## Posture Assessment

- Performs a scan of the devices connecting to a network for:
  - Antivirus definition updates
  - Registry settings
  - Windows or Linux updates – can be any operating system
- Allows the connection if device health is found as per the defined benchmark
- Denies access until:
  - Can alarm the user to fix the device with updates or missing definitions
  - Can redirect the device to a remediation server

## Penetration Testing

## Vulnerability Assessment

## Threat Assessment

Each network has several systems, servers, and networking devices. They form the overall posture for the network. However, the network posture needs to be assessed from time to time to ensure that regular antivirus or antimalware updates or Windows updates are taking place. It could also be that the registry settings on the systems are what they should be. Without the assessment, you cannot determine any of this.

When a system attempts to connect to a network, its security assessment can take place. If the system meets the security requirements, it is allowed to access the network. This is to ensure the security posture is kept intact and does not have any loose ends.

If the device or system does not meet the security requirements, it is denied access. In some cases, it is redirected to a remediation server, which covers the security gaps in the system.



# Business Risk Assessment – Process Assessment

Vendor Assessment

Process Assessment

- Works with the continuous goal in mind to improve existing:
  - Processes
  - Procedures
  - Policies
- Should be used if there are any amendments in the business functions or technological changes
- Can leverage new tools and techniques to improve the existing process

Processes become more and more critical as an organization grows. The processes are written keeping the business operations in mind. However, as users get used to the operations of their day-to-day jobs, they tend to miss out on the processes. This is quite normal. For example, the back up and restore process states that there must be a log entry for every backup and restore. The administrator may be particular about making the entry in the log, but he may just conveniently ignore it or forget about it after a while. Similar ignorance may appear in the other processes.

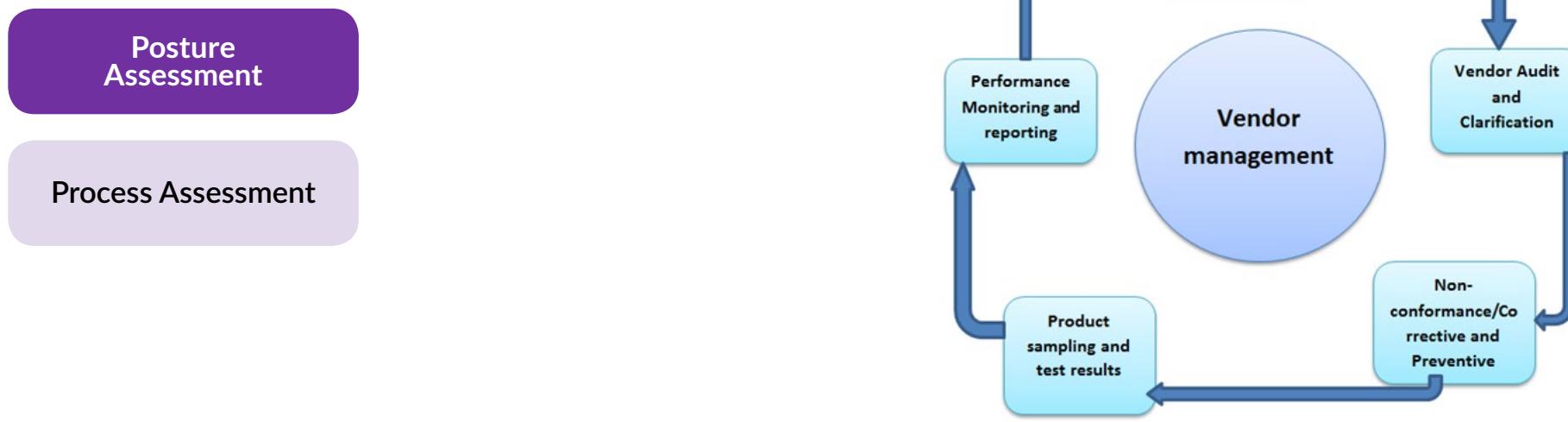
Policies are the overall guidelines from which the processes are created. One process can contain several procedures. A process ten can create several procedures. The distinction between processes and procedures is that a broad-level activities that need to be performed. On the other hand, procedures are instructions to perform a certain task. For example, a back and restore process can have two procedures – how to backup and restore.

Overall, the process assessment is used for continuously improving the policies, processes, and procedures. As and when there are operational changes, these need to be updated. For example, if you will not do tape backups anymore and will be doing cloud-based backups, you need to update the relevant policy, process, and procedures.

It is obvious that with technological advancements, several tools and techniques can be used to not only improve the processes but also to monitor them.



# Business Risk Assessment – Process Assessment



Every organization deals with vendors of different types. There can be vendors who supply raw material to your organization or an IT hardware supplier. From the business point of view, an organization may add several vendors, such as suppliers or service providers. However, adding more vendors also increases the security risks for the organization.

- To minimize the risk to the business and its operations, an organization should assess to evaluate the vendors. The assessment must include the following steps:
    - Evaluate the vendor profiles and perform a risk assessment
    - Perform a security audit and, if required, clarify points that may raise concerns or queries
    - Define corrective and preventive measures for the non-conformances that may arise during the vendor audit
    - Perform product sampling and evaluate the test results
    - Perform continuous performance monitoring and reporting



*TOPIC 11*

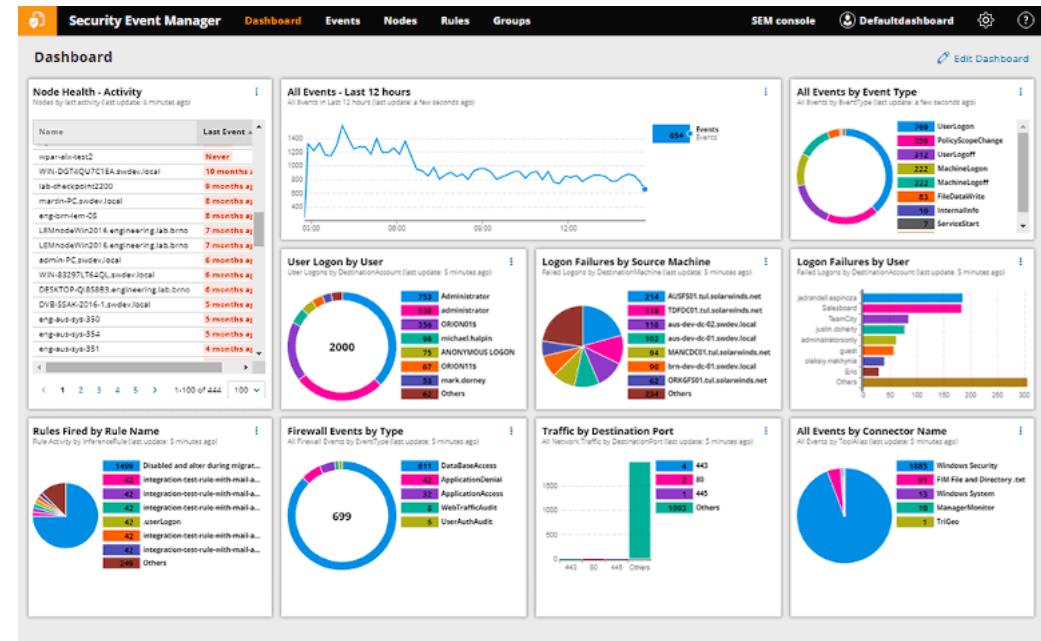
---

# SECURITY INFORMATION & EVENT MANAGEMENT

---

# Security Information & Event Management

- Is a tool that combines security information management (SIM) and security event management (SEM).
- Collates information from different devices and servers over the network
- Can perform various tasks, such as:
  - Event correlation
  - Alerts and notifications
  - Real-time log analysis
- Can be a hardware device or software
- Performs continuous monitoring of the environment



Many events can be generated in a network. The problem with the events is that you have to keep reviewing them manually and finding the relevant information, which becomes difficult. The solution to this problem is SIEM, which stands for Security Information and Event Management (SIEM). A SIEM combines Security Information Management (SIM), used for storing the events and generating reports, and Security Event Management (SEM), used for real-time monitoring of the events. It can perform various other tasks, such as data correlation and notifications.

A SIEM can collate events from different devices and servers on a network. This is not where its capability ends. Along with the collection of events, it performs real-time analysis of the events. With the capabilities built-in from SEM and SIM, the SIEM has some of the key features, such as:

- Event correlation: creates a relation between the events and alerts the administrator based on the rules that have been defined.
- Alert and notification: alert the administrator by sending notifications
- Real-time log analysis: can perform real-time analysis of the collated logs and highlights the critical events or events that require immediate attention

# Summary

- CIA Triad
- Threats
- Vulnerabilities
- Exploits
- Least privilege
- Role-based access
- Zero Trust
- Defense in depth
- Authentication methods
- Risk Management
- Security information and event management (SIEM)

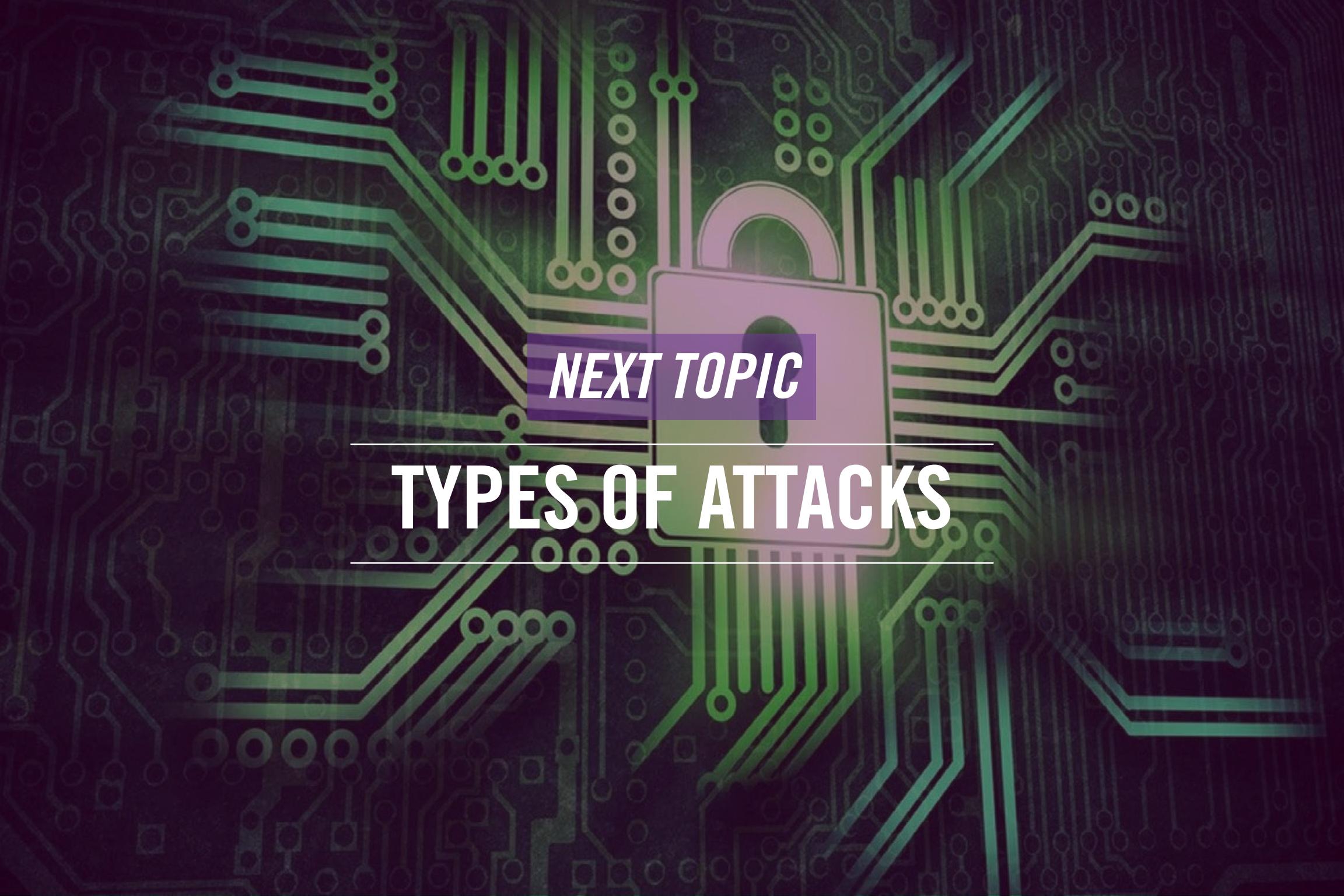


That's the end of the lesson.

Here we covered:

- |  |   |
|--|---|
| <ul style="list-style-type: none"><li>• CIA Triad</li><li>• Threats</li><li>• Vulnerabilities</li><li>• Exploits</li><li>• Least privilege</li><li>• Role-based access</li></ul> | <ul style="list-style-type: none"><li>• Zero Trust</li><li>• Defense in depth</li><li>• Authentication methods</li><li>• Risk Management</li><li>• Security information and event management (SIEM)</li></ul> |
|--|---|





*NEXT TOPIC*

---

# TYPES OF ATTACKS

---

Lesson

1

---

# Types of **Attacks**

- 1 — Welcome to the first lesson of Module 4. In this lesson, you will learn about the:
  - 2 — Explain Common Security Concepts
- 



Network Fundamentals

# Agenda

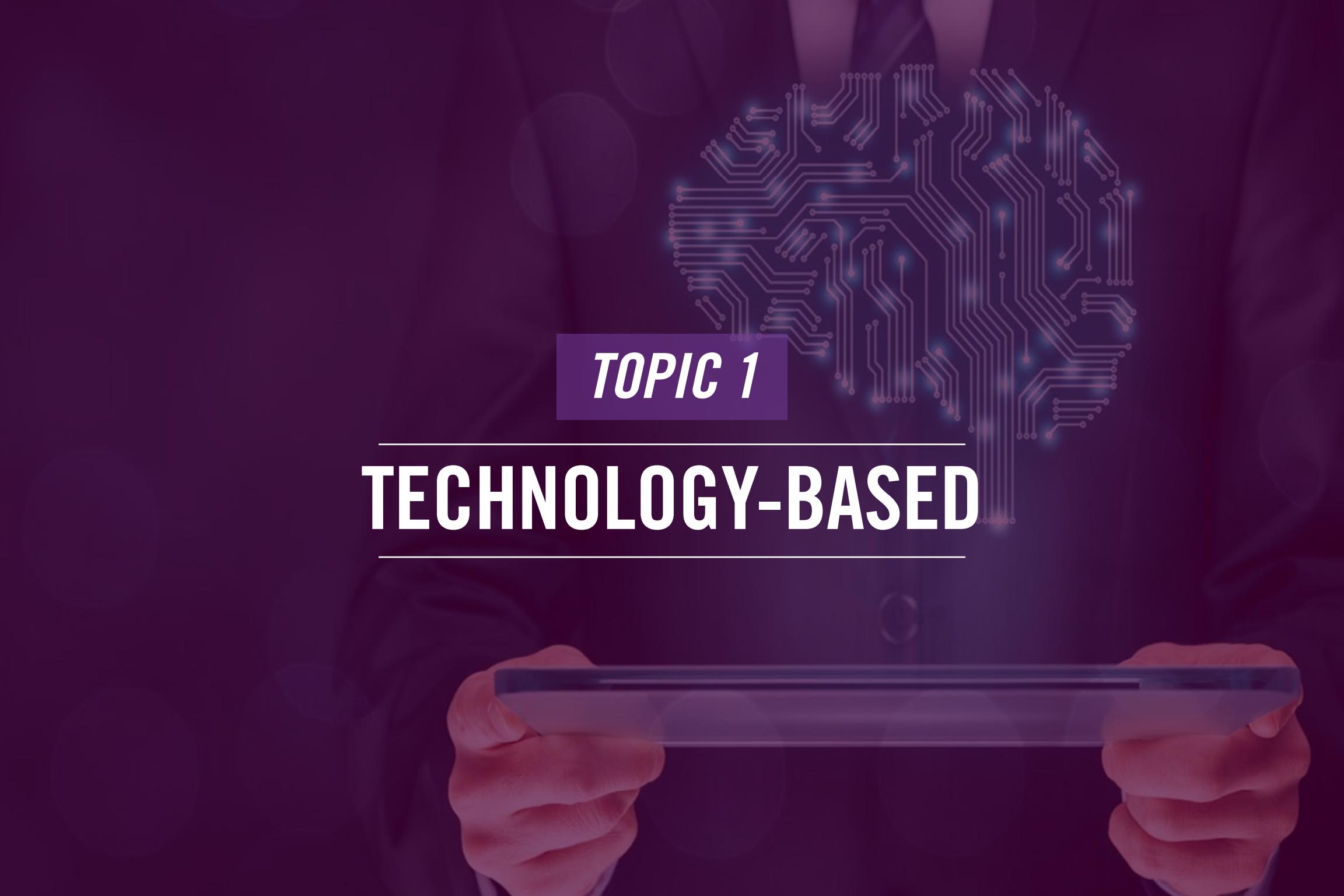
- Technology-based
- Human and Environmental



Hi, welcome to COMPTIA Network+ Course  
In this lesson, we will talk about:

- Technology-based
- Human and Environmental





*TOPIC 1*

---

# TECHNOLOGY-BASED

---

# DoS/DDoS

- DoS
  - Stands for Denial-of-Service
  - Prevents users from accessing network services
  - Is performed by a single system
  - Is usually targeted to a Webserver
- DDoS
  - Stands for Distributed Denial-of-Service
  - Is the amplified version of DoS
  - Is conducted using hundreds or thousands of systems that are controlled by the attacker



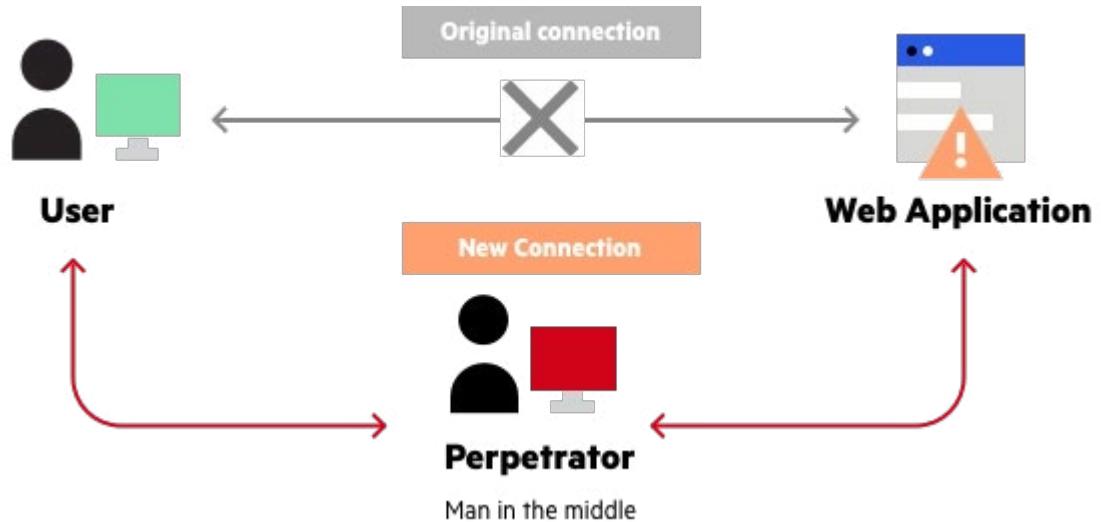
The first type of technology-based attack is the Denial-of-Service, known as DoS. A DoS attack is conducted to prevent the users from accessing specific resources, such as a website. For example, let's say that you have a website, and a DoS attack is launched against it. The web server receives a large number of requests that it has to respond to. In responding to these requests, the webserver exhausts its resources and stops responding to legitimate requests from the users.

A DoS attack is conducted using a single system, which can send a large number of requests. The same is applicable for any other type of server, such as a file server. In most cases, a DoS attack is targeted to a webserver. However, depending on the webserver's resources, it may take a while for the webserver to go down.

Now that you know about a DoS attack, the DDoS or Distributed Denial-of-Service attack is an amplified version of it. Instead of using a single system to launch the attack, DDoS uses hundreds or thousands of systems, which are bots or zombies, to conduct the attack. There is a command-and-control center that the attacker uses to control these bots or zombies. Think of this: if one system can impact a webserver and bring it down, it is difficult for any system to stand against a DDoS attack if the same is multiplied by thousands of systems.

# On-path attack

- Is also known as Man-in-the-Middle attack
- Intercepts packets from a communication taking place between two parties
  - Both the parties don't know
- Focuses on stealing the information
- Works with the following phases:
  - Interception of traffic
  - Decryption of traffic



The On-path attack was earlier known as the Man-in-the-Middle attack. In this attack, an attacker intercepts the packets from communication between two users or a user and an application. In the process of an on-path attack, both parties are unaware of an interception taking place. So, the attacker can conveniently intercept the packet and either alter the information or even steal it.

The on-path attack is divided into two parts. The first part is the interception, in which an attacker can use various methods to conduct the on-path attack. Some of the common methods are:

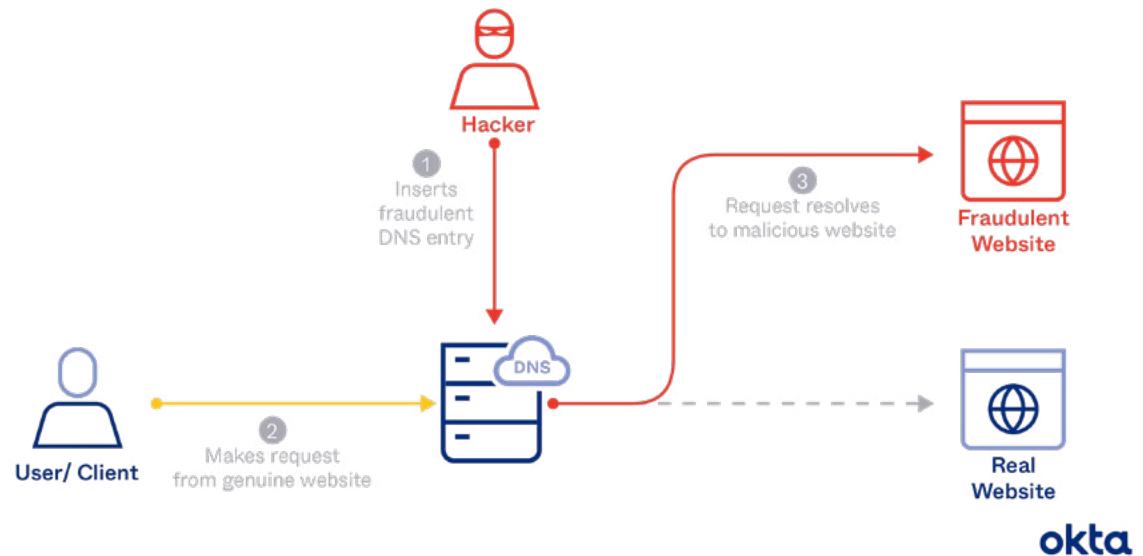
- IP spoofing: by using the IP address of the source system.
- ARP spoofing: by using the MAC address of a legitimate system on the network
- DNS spoofing: by altering the DNS record and changing the address of a website to redirect the traffic to a fake website

The second part is the decryption of the traffic. The captured traffic may be encrypted using SSL that requires decryption. It can be done using various methods, such as:

- HTTPS Spoofing: by embedding a fake certificate into the client's web browser
- SSL Beast: by exploiting a vulnerability in TLS 1.0 and capturing the encrypted cookies that are decrypted by compromising the cipher block chaining (CBC)
- SSL Hijacking: bypassing forged authentication keys to both parties, the client and application
- SSL Striping: by downgrading the HTTPS connection to HTTP

# DNS Poisoning

- Is conducted by updating the DNS record to redirect the requests to a wrong address
  - Wrong address is the address of a fake website
  - Users are redirected to the fake website
- Helps the attacker to gain user credentials when entered on the fake website
- Occurs if DNS server is insecure



In a typical DNS scenario, a client sends a request to resolve a hostname or a website name. The DNS server, if authoritative, responds to the client's request on its own. Else, it forwards the request to the authoritative DNS server for the website or hostname. After a response is received, the DNS server performs two tasks:

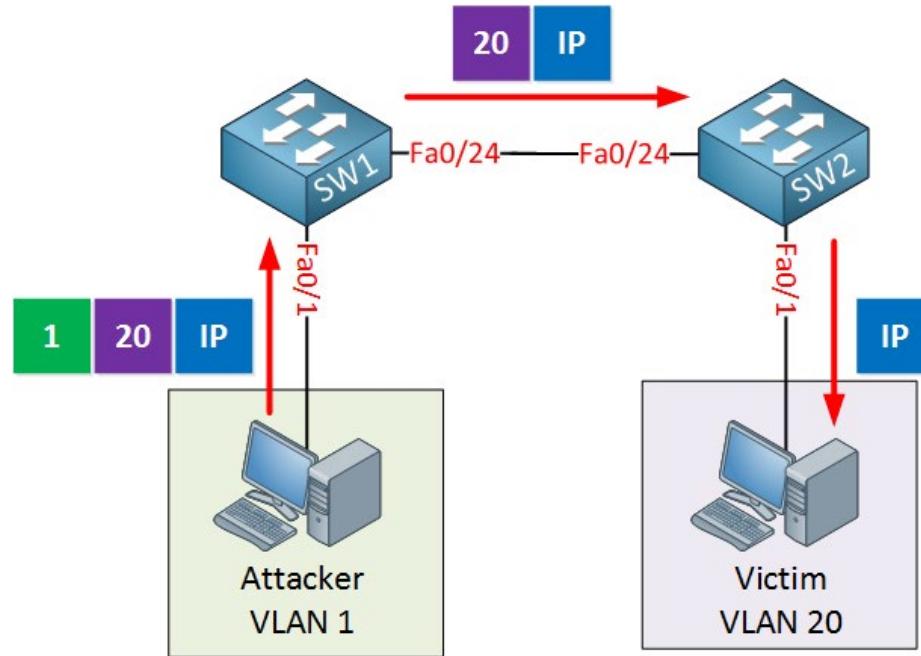
- Responds to the client with the answer
- Caches the result for a specific time, such as an hour, which is the Time To Live (TTL)

This is the normal process. However, in the DNS cache poisoning or DNS poisoning attack, things change slightly. The attacker updates the DNS record with the wrong address. Let's say the record for google.com was cached and had an IP address of 8.8.8.8. The attacker will change the IP address to 1.1.1.1, which is hosting a replica of the google.com website and is maintained by the attacker. When a user attempts to access google.com, the DNS server redirects the request to 1.1.1.1 instead of 8.8.8.8. For the user, this process is transparent.

When a user attempts to log on to google.com by entering user credentials, which is a fake website, the attacker collects the user credentials. This type of attack occurs when a DNS server is insecure, which means accepting the update requests from any DNS server. You should restrict it to receiving updates from specific DNS servers.

# VLAN Hopping

- Is an attack in which an attacker can send a VLAN traffic to another VLAN
- Can be conducted using two different methods:
  - Double tagging
  - Switch spoofing



A network is typically divided into virtual LANs or VLANs. A VLAN is:

- It is a logical division of ports on a switch
- Can span across multiple switches by using a trunk link

The traffic needs to be restricted within a VLAN. One VLAN traffic should not be overflowing with the traffic of other VLANs. This control is implemented using access control lists or ACLs.

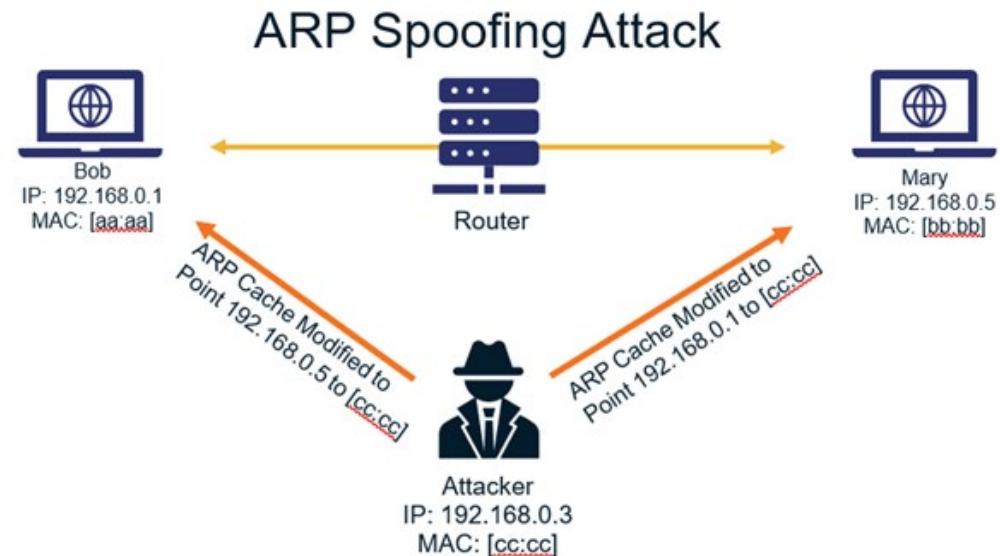
An attacker makes use of a packet sniffing application. In the VLAN hopping attack, the attacker can send the traffic from one VLAN to another VLAN even if the access control lists are applied. The attacker is also able to gain access to the traffic from other VLANs.

To conduct a VLAN hopping attack, an attacker can use one of the two methods:

- Double tags: the attacker adds the address of the target VLAN as the outer VLAN tag and the address of the native VLAN as the inner VLAN tag. After receiving the frame, the switch removes the inner VLAN tag and forwards the frame to the target VLAN.
- Switch Spoofing: the attacker negotiates the trunk with the switch, using either dynamic auto or dynamic desirable configuration. After the attacker gains access to the trunk, the attacker can gain access to all VLANs.

# ARP Spoofing

- Is performed by sending falsified ARP messages over a network
- Links the attacker's MAC address to an IP address of a real system on the network
- Is used to perform malicious tasks, such as:
  - Intercept data
  - Modify data
- Can be used to conduct attacks, such as:
  - DoS
  - Session hijacking
  - Man-in-the-Middle



Each system maintains an ARP cache that contains the mappings of IP addresses with their respective MAC addresses. The ARP spoofing attack is the method of sending falsified ARP messages over a network. Remember that you had learned that switches mainly rely on the MAC addresses. When the attacker learns the MAC address of a device, he uses the same MAC address for his system. In this scenario, when the traffic was destined for a specific MAC address, now being used by the attacker's system, it is redirected to the attacker.

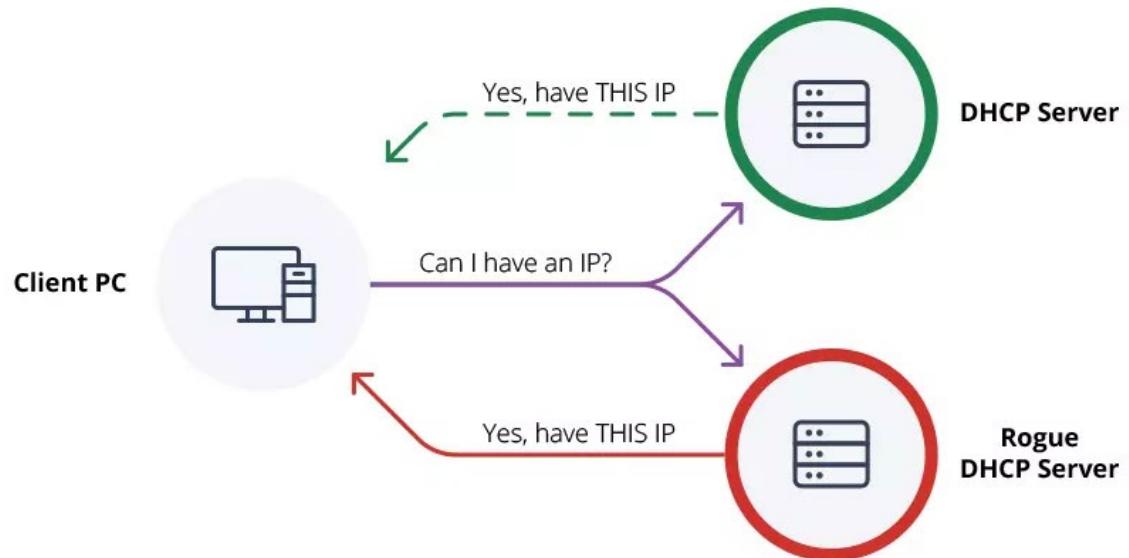
On the other hand, the attacker's MAC address can also be linked to an IP address that belongs to another system on the network. The result is the same. The attacker is still able to poison the ARP cache. In short, the attacker can intercept data and modify the data as well. The end-users or both parties do not know that there is an interception of the data.

ARP spoofing is used with various types of attacks. Some of the common attacks are:

- Denial-of-service: by linking several IP addresses to a single MAC address that belongs to the target system. All the traffic intended for these IP addresses is now sent to the target system and overwhelms it
- Session hijacking: by stealing session IDs that allows the attacker to gain access to the sessions to steal data
- Man-in-the-middle: by intercepting the traffic between two parties

# Rogue DHCP

- Is an unauthorized DHCP server that leases IP addresses to the client systems
- Leases incorrect information, such as:
  - IP address
  - Subnet mask
  - Default Gateway
  - DNS server



Networks rely on DHCP servers to lease IP addresses to the client systems. In most cases, a midsize network of 200-300 systems will have a single DHCP server or two or more for redundancy purposes. These are considered to be authorized DHCP servers that lease IP addresses. The rogue DHCP server works similarly to the legitimate DHCP server. It leases the IP addresses to the client systems, which don't know whether it is a legitimate DHCP server or a rogue one.

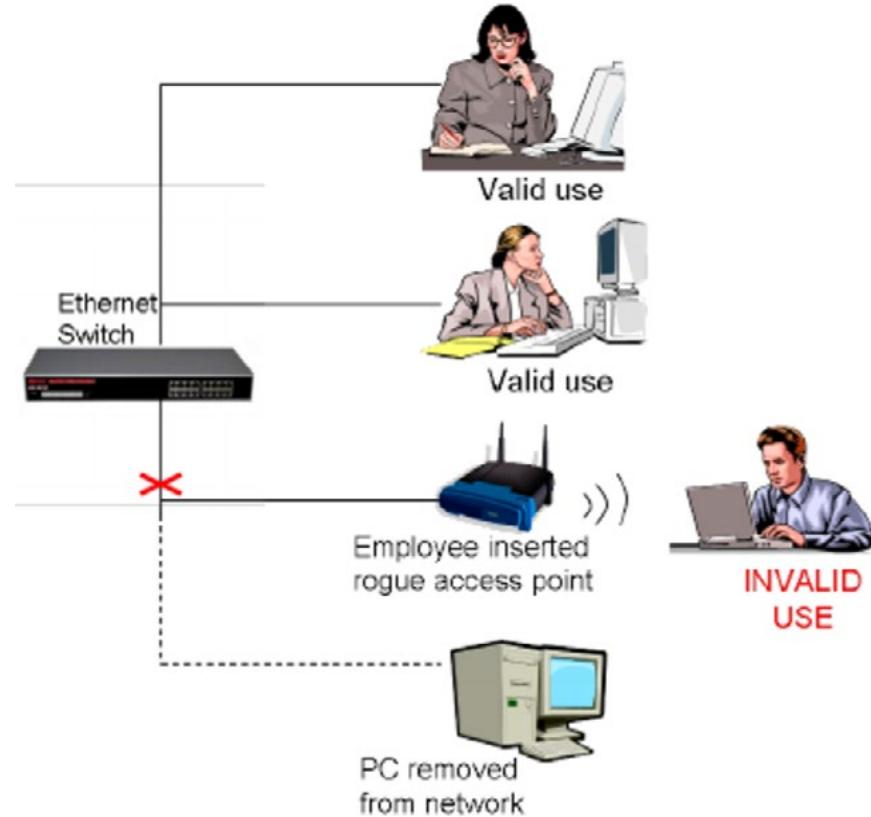
A rogue DHCP server performs the IP leases in the usual manner. It leases the following:

- IP address
- Subnet mask
- Default Gateway
- DNS server

The fundamental problem with the rogue DHCP server is that it can allow the attacker to provide the DNS server that contains altered DNS records. For example, it can use an IP address to redirect the user to a fake website to access their credentials.

# Rogue Access Point (AP)

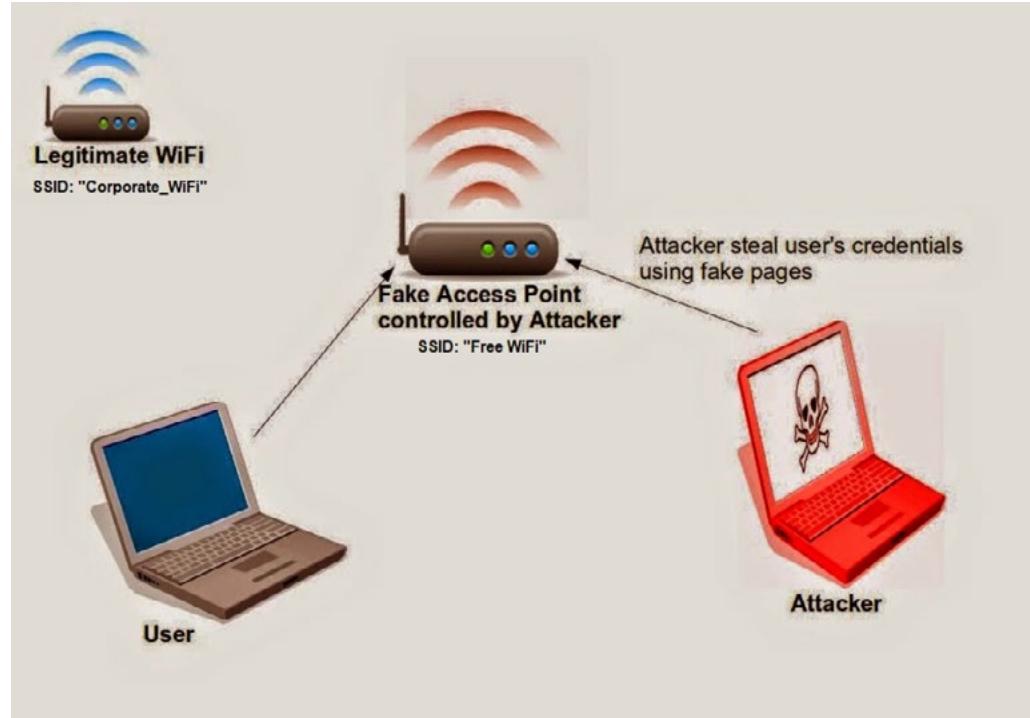
- Is an unauthorized access point placed into a network
- Can be intentional or unintentional
  - Intentional: Is set up by an attacker to get
  - Unintentional: A user may set up an access point to use wireless network



A rogue access point or an AP is an unauthorized access point that is placed into the network. Sometimes users, for the sake of their convenience, might set up an access point to gain wireless access. Their intention is not wrong. They unintentionally added a security threat by putting an AP into the network. On the other hand, a hacker may have wrong intentions, such as conducting peer-to-peer attacks to gain information from the client. To do this, the attacker launches the deauthentication attack to remove the wireless clients from the legitimate AP and then leaves its AP open so that the wireless clients can discover and connect to it.

# Evil Twin

- Is a form unauthorized wireless access point on a network but with a similar name as an authorized AP
- Requires no password for connecting to the AP
- Is used to conduct peer-to-peer attack
- Allows the attacker to force the clients off the legitimate AP
  - Clients get disconnected from the legitimate AP
  - Clients search for the AP and find another AP with the same name
  - Clients connect to the evil twin AP
  - Attacker initiates the peer-to-peer attack



An evil twin is just a rogue AP that is made available. However, it uses the same name as the legitimate or the authorized AP. The attacker's AP is configured with the evil twin without any authentication method, such as a password. The attacker uses the evil twin to conduct a peer-to-peer attack.

The attack starts with putting an AP with a similar name as the legitimate AP. After setting up the evil twin AP, the attacker launches the deauthentication attack to get the clients disconnected from the legitimate AP. After the clients are deauthenticated, they search for the same AP and encounter the evil twin AP, which does not have any authentication and is open. The clients then connect with the evil twin AP – thinking that this is the legitimate AP. Now, the attacker has access to all the connected clients and can launch the peer-to-peer attack.

# Password Attacks – Brute-force

Dictionary

- Is a type of password cracking method
- Uses different combinations of letters, numbers, and special characters to crack a password
- Works with millions or billions of password combinations
- Can crack easy passwords in minutes whereas the complex and long passwords may take years

Brute-force

In most cases, users secure their login accounts with a password. In some cases, an organization may also set up two-factor or multi-factor authentication, but the password is still the only factor for authentication being used.

A password can always be cracked. The first method is the brute-force method. In this method, an attacker uses a combination of letters, numbers, and special characters to crack the password. For example, let's assume that the attacker uses the following:

- Upper and lowercase letters – A to Z and a to z
- Numbers – 1 – 10
- Special characters - ~!@#\$%^&\*(),.
- Length of the password – something like 8 characters that include the combination of letters, numbers, and special characters

With the help of specialized tools, the attacker selects this combination to crack the password. There can be a possibility that the tool may have to try millions or billions of combinations before the actual password is cracked.

An easy password can be cracked without much effort. For example, the password is James. The password cracking tool will take a few minutes to crack this password using the brute force method. The most widely used password, 'password,' is cracked in a second. Therefore, it is always recommended to use a complex password. Long and complex passwords may take years to crack.



# Password Attacks – Dictionary

## Dictionary

- Is also a password cracking method
- Uses a dictionary to crack the password
- Is performed using a specialized tools
  - Can use the built-in dictionary
  - Can use the dictionaries available on the Internet
- Requires time and processing power

## Brute-force

Dictionary is another password cracking method. A dictionary, a long list of words, is used to crack the password in this method. Each word is compared with the password until the real password is discovered or cracked.

There are several password cracking tools that support the dictionary method. Most of them carry their custom dictionary that can be used. However, you are free to browse the Internet and download more dictionaries.

The dictionary and brute-force methods require time and a lot of processing power. If you have a high-end system with many resources, like 16 GB memory, it will speed up the process, but in the end, it all depends on the kind of password you use. If it is easy, the attacker may just get the password cracked in a few minutes.



# MAC Spoofing

- Is using another system's MAC address for a malicious purpose
- Can be performed for various reasons, such as:
  - Anonymization
  - Identity Theft
  - Licensing Terms
  - Receive data that is meant for another system
- Can be performed manually or using a tool, such as:
  - Technitium MAC Address Changer
  - Win7 MAC Address Changer



MAC spoofing is another type of attack. In the MAC spoofing attack, you use a MAC address and assign it to your system. Let's take an example – your system does not have access to the wireless network that has MAC filtering enabled. Your colleague's system can connect to the wireless network. You use his system's MAC address and assign it to your system. Now, your system can access the wireless network.

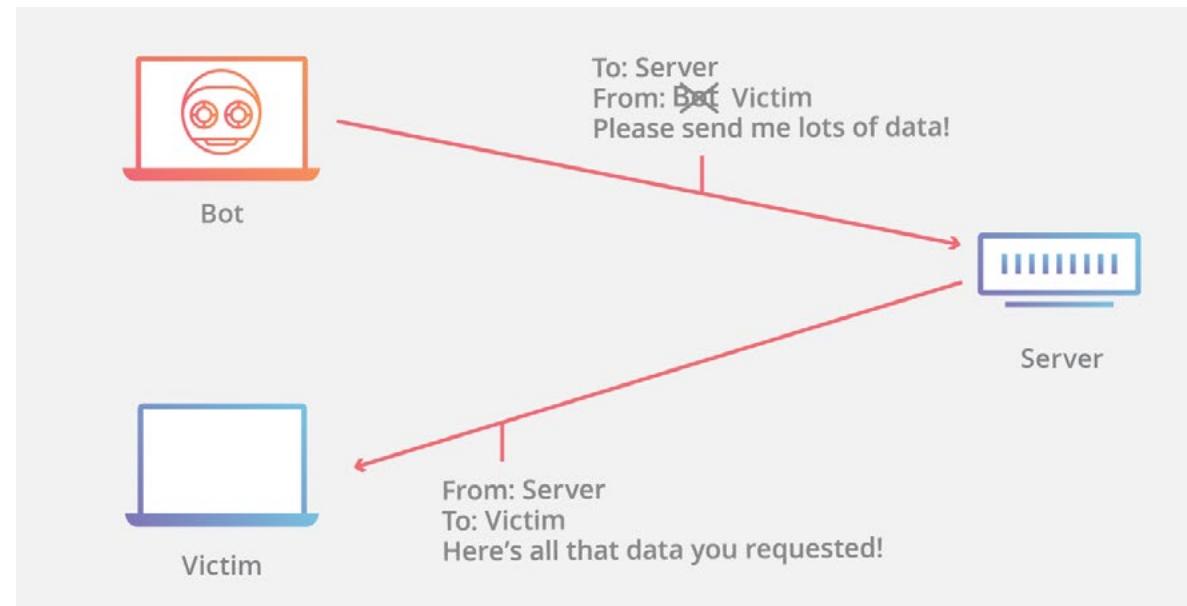
It is obvious that the MAC spoofing does not have a legitimate intent – there has to be a malicious intent that could be:

- Anonymizing the attacker's system – your real MAC address is hidden as you spoofed it
- Identity theft – you are using someone's MAC address – it is identity theft of a system
- Licensing terms – you can violate the licensing terms if they do not allow your MAC address to access an application. With a known MAC address, you can spoof to get access.
- Receiving data that is meant for another system – you use someone's MAC address to receive data that was intended for the original recipient

MAC Spoofing can either be performed manually. For example, you can go into the network adapter's properties in Windows and change the MAC address. It can also be done via tools like Technitium MAC Address Changer and Win7 MAC Address Changer.

# IP Spoofing

- Changes the IP address of a system to:
  - Hide the identity of a system
  - To impersonate another system
  - To pass through a firewall acting like another system
  - To conduct an attack like DDoS

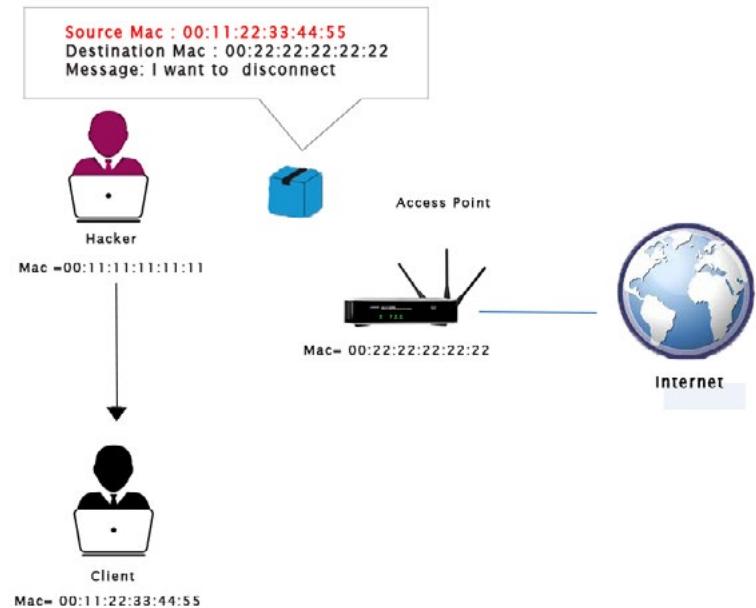


IP spoofing is using some other system's IP address to perform malicious tasks, such as:

- Hide the identity of a system – if an IP is allowed access, you can spoof with an allowed IP address
- To impersonate another system – to receive data
- To pass through a firewall acting like another system – if the spoofed IP address is allowed access, then you will be allowed to pass through the firewall
- To conduct an attack like DDoS – so that the real IP address cannot be tracked

# Deauthentication

- Is a type of DoS attack
- Focuses on the wireless router and the connected clients
- Requires the attacker to send deauthentication frame to the wireless access point
  - Attacker needs to know the client's MAC address
- Is used for attacks like:
  - Evil access point
  - Password attacks



Deauthentication attack is a type of denial-of-service or DoS attack in which the attacker sends a large number of packets to the access point. The Deauthentication attack mainly works with the wireless networks where a client with a spoofed MAC address sends a deauthenticaiton packet. The AP or the wireless router receives the packet and disconnects the client.

In this process, the attacker has first to find the client's MAC address. Without knowing the MAC address, it is not possible to conduct the Deauthentication attack. Attackers usually use a tool called aireplay-ng to launch the Deauthentication attack.

The Deauthentication attack works like a precursor for attacks like Evil twin and password cracking. In the evil twin, when the clients are deauthenticated, they connect to the evil twin with the same name as the legitimate AP to which the clients were connected.

In the password attack, the attacker sniffs the WPA handshake traffic. This can be done by deauthenticating the client, which then attempts to connect again. You can then capture their credentials using a man-in-the-middle attack.

# Malware

- Is the full form of Malicious Software
- Can perform various actions, such as:
- Delete data
- Corrupt system files
- Convert a system to a zombie
- Spread through the network to impact its performance
- Has various types, such as:
- Virus
- Worm
- Trojan
- Ransomware



Malware stands for malicious software, which is designed with the wrong intentions. Different types of malware perform actions like:

- Delete data
- Corrupt system files
- Convert a system to a zombie
- Spread through the network to impact its performance

The type of actions a malware performs depends on the way it has been designed. Different types of malware behave differently and impact a system in different ways. For example, a worm will traverse through the network and impact its performance. Let's understand a few common types of malware:

- Virus
- Worm
- Trojan
- Ransomware

These are just a few types. Other types are spyware, adware, key logger, and rootkits.

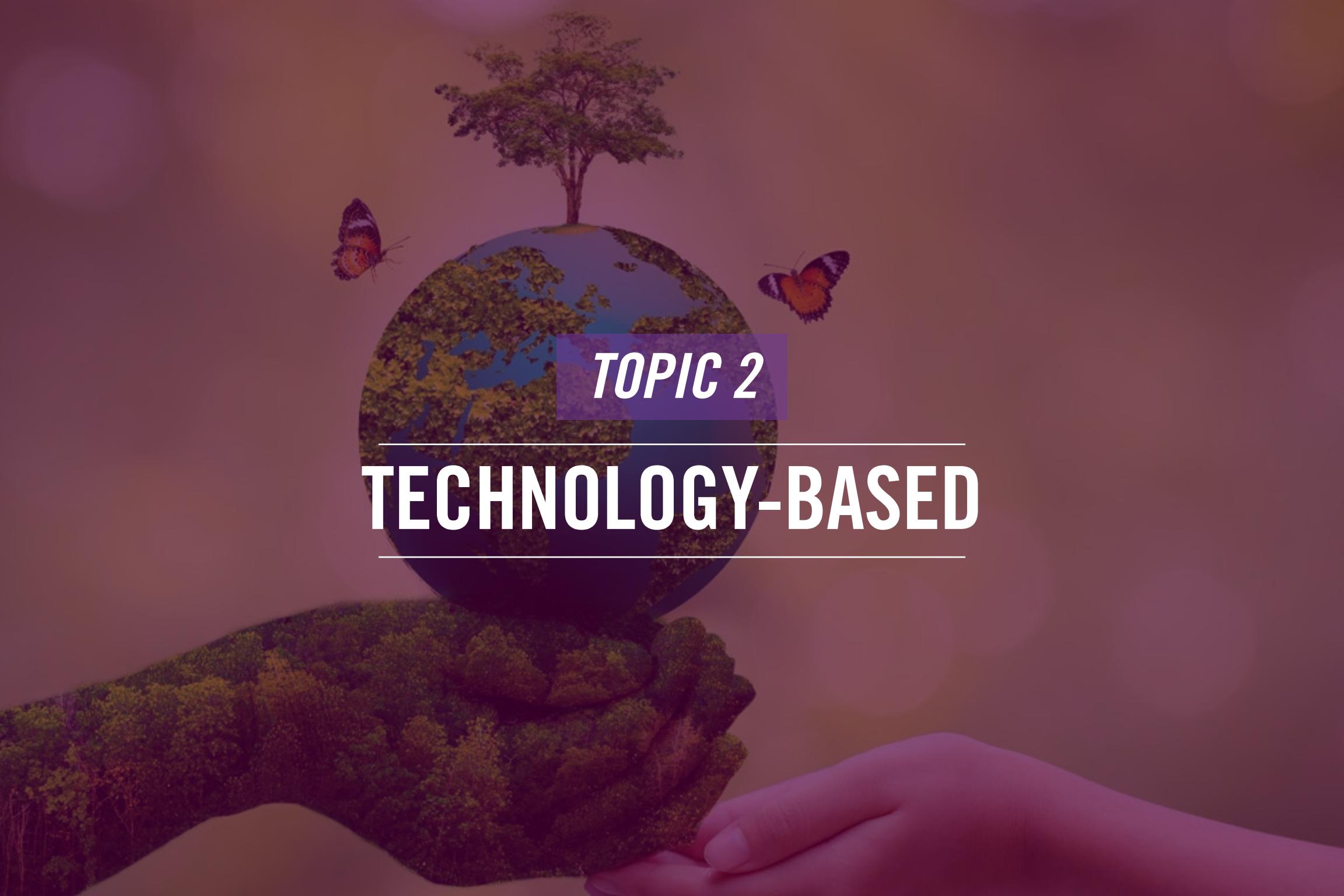
# Ransomware

- Is a type of malware
- Encrypts the user's data and prevents access
- Holds the user for a ransom
- Private key is with the attacker
- May or may not be given to the user even after the ransom is paid



Ransomware is a type of malware that encrypts the user's data. After the data is encrypted, the user is unable to open any of the encrypted files. The attacker now has access to the entire encrypted data. In this case, a message is displayed to the user that the user has to pay a certain amount of ransom to decrypt the data. It can also be possible that the user's entire system is encrypted and when the user boots into the system, a message is flagged for ransom. In either case of the system or data, the attacker demands the ransom as he holds the private key that can decrypt the data.

There is no guarantee that even if the user pays the ransom, the attacker will decrypt the system or the data. The ransom is demanded in the cryptocurrency – mostly the bitcoins.



**TOPIC 2**

---

**TECHNOLOGY-BASED**

---

# Phishing

Shoulder Surfing

- Is a type of social engineering attack
- Involves a real-lookalike website (replica of a real website) and a well-crafted email
- Pretends that the email from a known source, such as bank

Piggybacking

Tailgating

Phishing

- Website is replica of the bank or any legitimate source mentioned in the email
- Requires the user to click on the given link
- User clicks on the link to enter personal information, such as username and password
- Attacker captures the information

Phishing is one of the most commonly used social engineering attacks in existence today. If you have ever received an email asking you to reset your password for your account in Bank of America, you can assume it is a phishing email. You know that is a phishing email because you do not have an account with Bank of America.

Phishing involves two key components:

A well-drafted email that contains a link to a fake website

A fake website that looks the same as its original counterpart but is hosted by the attacker

The phishing email tries to attract or scare the recipient to act quickly without thinking twice. The intent is to get the user to click on the link within the email. If the user does that, the user is taken to the fake website, where the user enters the user credentials. The attacker captures the user credentials.

In some cases, the phishing email may prompt the user to click on the link within the email, but instead of a fake website, the user is taken to a malicious website that drops malware onto the user's system. The attacker uses the malware to either steal the data or use the system as a bot or zombie to conduct a DDoS attack.

# Tailgating

Shoulder Surfing

Piggybacking

Tailgating

Phishing

- Is following an authenticated user through a door without authenticating himself or herself
  - A user authenticates by swapping a card or entering a PIN
  - Another user follows without authentication
- Is hard to prevent unless security measures are put in place:
  - Mantrap
  - Guard

Tailgating is a problem that is faced by almost every organization. Tailgating involves two or more entities. The first entity is authenticated to enter a door, and the second entity follows without authenticating itself. The second user has tailgated the first user to enter into the room or the building.

In some cases, it is unintentionally performed by the users, but in some cases, an attacker may want to get into the building to have physical access to the network or its resources. Tailgating is hard to prevent, but organizations use guards or mantrap to prevent tailgating.

# Piggybacking

Shoulder Surfing

**Piggybacking**

Tailgating

Phishing

- Is similar to tailgating with a slight difference
  - Tailgating: Authenticated user does not know someone is entering the door right behind him or her
  - Piggybacking: Authenticated user knows someone is entering the door right behind him or her
- Requires security controls similar to tailgating

Piggybacking is similar to the tailgating method. It also lets an unauthenticated person pass through a door that an authenticated user opened. Piggybacking has one key difference from tailgating.

- Tailgating: Authenticated user does not know someone is entering the door right behind them
- Piggybacking: Authenticated user knows someone is entering the door right behind them

Just like tailgating, you can use a guard or mantrap to prevent piggybacking.



# Shoulder Surfing

## Shoulder Surfing

- Is watching over someone's shoulders when they are working on their system
- Is performed with the intent to read through information, such as:
  - Password
  - Social security number
- Can happen with anyone anywhere
- Can lead to an identity theft

## Piggybacking

## Tailgating

## Phishing

Have you ever had someone standing behind you when you were working? If yes, then this person was performing shoulder surfing. In shoulder surfing, a user stands behind another user to read through the content, which might be confidential.

For example, let's say that you have opened a web browser to access your bank account. Your colleague sneaks right behind you and sees your account number and password typed on the keyboard. Your colleague is shoulder surfing in this scenario.

Shoulder surfing intends to read or see confidential information, such as your password, social security number, or even a bank account number.

Shoulder surfing is a common type of attack that can happen to anyone anywhere. For example, it can happen when you are working on your laptop in a café. The information gained by the person can lead to an identity theft attack.



# Summary

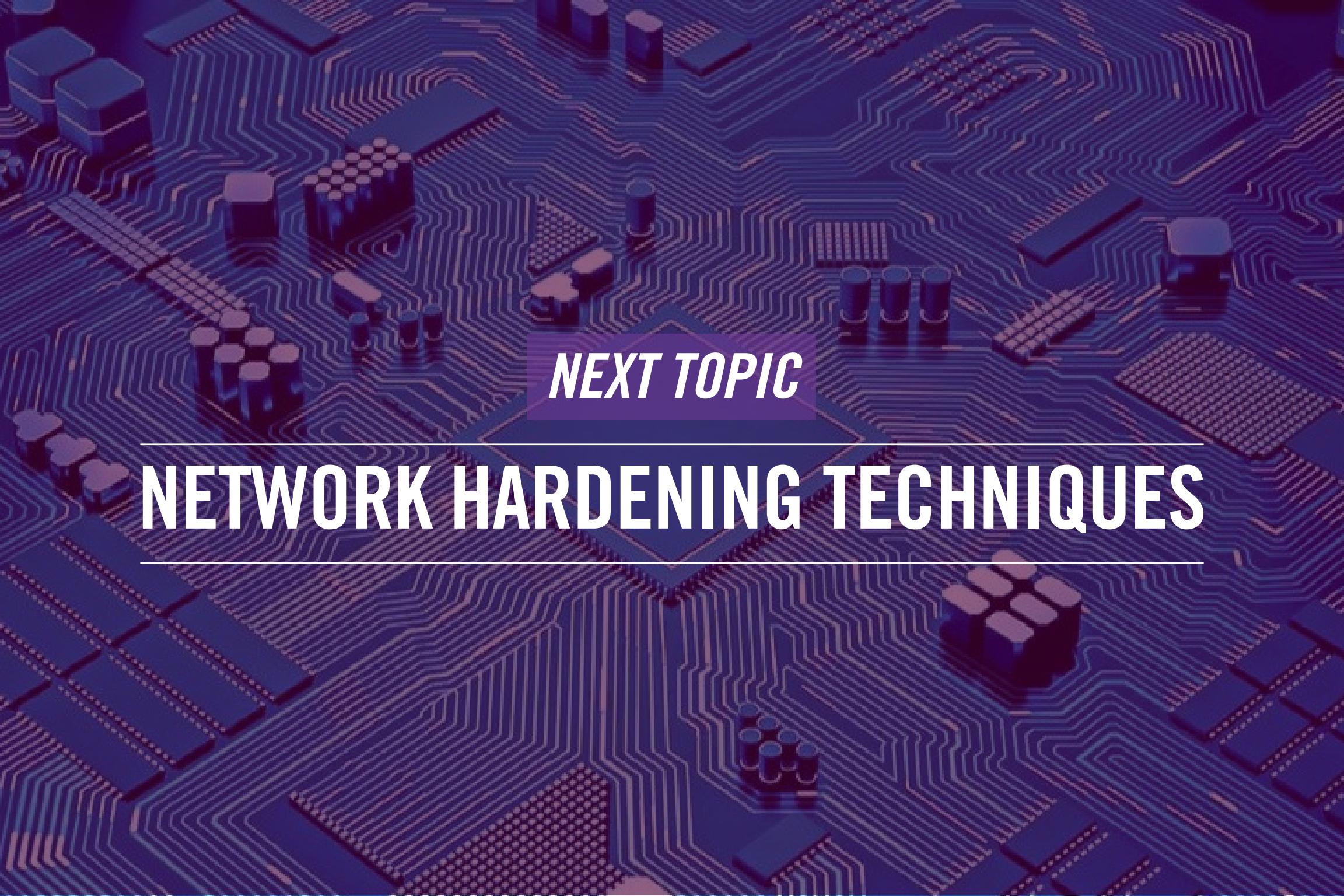
- Technology-based
- Human and Environmental



Hi, welcome to COMPTIA Network+ Course  
In this lesson, we will talk about:

- Technology-based
- Human and Environmental





**NEXT TOPIC**

---

# NETWORK HARDENING TECHNIQUES

---

Lesson

# 3

---

# Network Hardening Techniques

- 1 — Welcome to the 3 lesson of Module 4. In this lesson, you will learn about the:
  - 2 — Explain Common Security Concepts
- 



Network Fundamentals

# Agenda

- Best Practices
- Wireless Security
- IoT Access Considerations



Hi, welcome to COMPTIA Network+ Course

In this lesson, we will talk about:

- Best Practices
- Wireless Security
- IoT Access Considerations





**TOPIC 1**

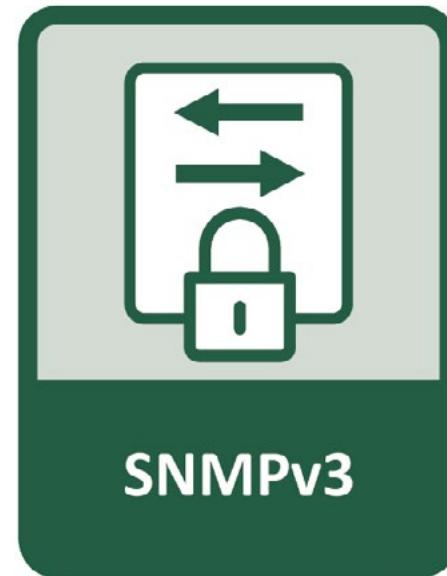
---

# BEST PRACTICES

---

# Secure SNMP

- Use SNMPv3 that encrypts the messages between agents and managers to maintain:
- Confidentiality
- Integrity
- Uses Transport Security Model (TSM) to apply security at the Transport layer of the OSI model
- Uses asymmetric cryptography



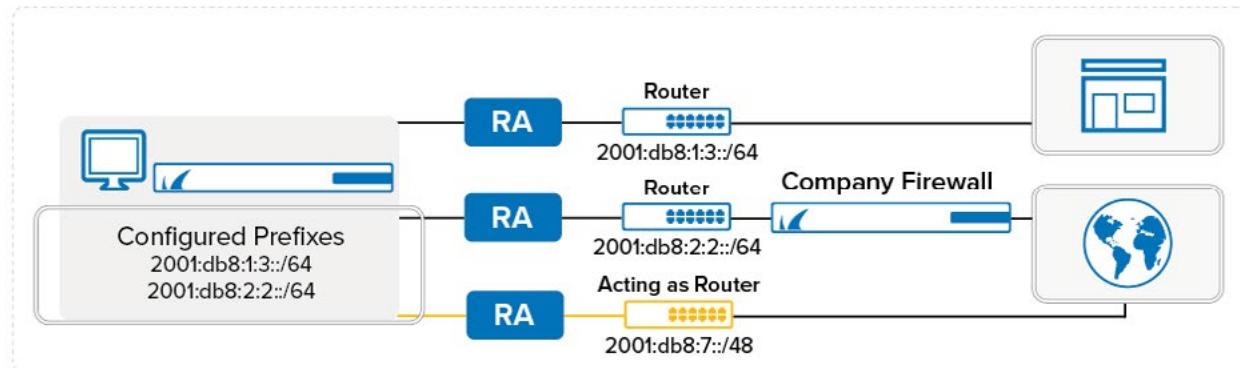
SNMP or Simple Network Monitoring Protocol is used for monitoring the network devices. For example, a router or switch configured with SNMP can send its status update to a server and inform that it is live on the network. SNMP has three versions – v1, v2, and v3. The first two versions had many security flaws that are now taken care of in SNMPv3.

One of the major improvements in SNMPv3 was the addition of encryption. Unlike the SNMPv2, which performed community-based authentication, SNMPv3 can perform user and group-based authentication. It can perform DES, SHA, MD5, and AES-based encryption on the messages that are being shared between the agents and managers. With the encryption, it can maintain the confidentiality and integrity of the messages.

It also uses Transport Security Model (TSM) component to apply security at the Transport layer. It uses protocols that are based on asymmetric cryptography.

# Router Advertisement (RA) Guard

- Is a feature of IPv6 and is part of Network Discovery Protocol (NDP)
- Replaces ARP in IPv4
- Accepts or rejects rogue RA Guard messages
- Accepts only if the RA frame contents are validated
  - Checks for source Link Layer address and Prefix information



The routers use router advertisements for neighbor discovery. If anyone gets hold of these packets, it could reveal much information about the routers. To prevent this from happening, a new method can be used. This method is known as Router Advertisement (RA) Guard, which is a feature of IPv6. With the RA Guard, the network administrator can choose to accept or reject the router advertisements.

In the IPv4, ARP messages were used. However, in IPv6, ARP messages are now replaced with the router advertisement, which is multicast messages. These messages help the routers announce their state to their neighbors. The NDP protocol uses these messages for finding the neighbors.

RA messages are prone to spoofing attacks as they are unsecured by default. To prevent such attacks, you need to use the RA Guard feature. It prevents the use of rogue RA messages from unauthorized entities. When a RA message is received, the RA Guard validates the message based on several parameters, such as:

- Source MAC address
- Source IPv6 address
- Source IPv6 address prefix
- Hop-count limit

If the RA messages meet the criteria, they are forwarded to the destination. If the message does not meet the criteria, then they are rejected.

# Port Security

- Is a network hardening method
- Works at Layer 2 of the OSI model
- Prevents an ad hoc device to connect to a port
- Restricts specific MAC addresses on switch ports
- Can restrict only one or more MAC addresses to connect to a port



In most cases, a switch will have several ports that are available and free for use. These ports can be misused if they are not appropriately secured. For example, anyone can plug a malicious laptop into the port and release malware or capture network traffic. To secure the free ports, you need to configure port security, mapping one or more MAC addresses with the specific ports.

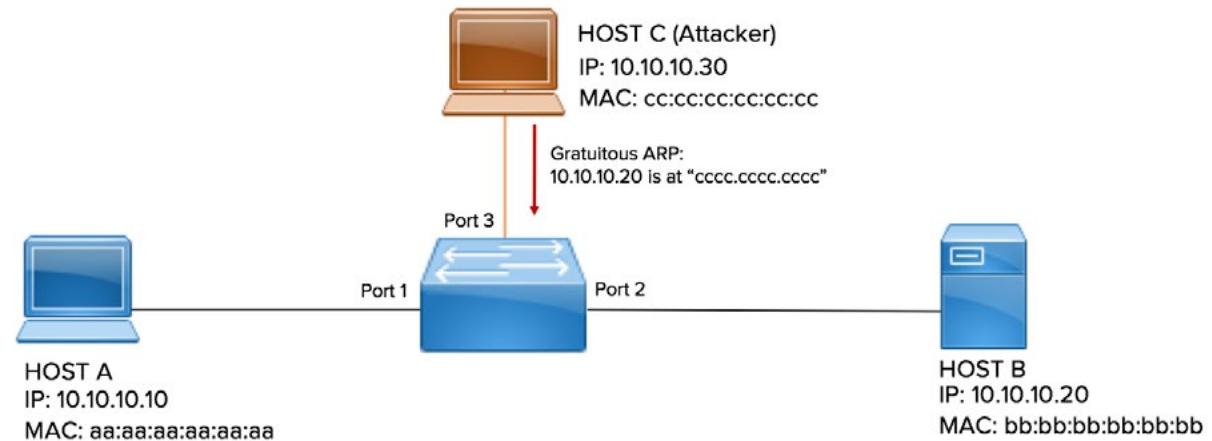
Port security works at the Data Link Layer, which is Layer 2 of the OSI model. Port security requires the use of managed switches, which the administrator configures for better control and usage of the switch. With the port security, you can limit which MAC addresses can use a specific port. You can also increase the port security by disabling them when they are not in use.

It is also essential to understand that the administrator can configure different actions for port security. For example, if a violation of any kind involves a port, it can be shut down automatically.

In the given graphic, only two MAC addresses are allowed to connect to a port. Therefore, the third MAC address, which belongs to Host B, is denied access.

# Dynamic ARP Inspection

- Uses IP-address-to-MAC address mapping for MAC verification of each frame
- Uses the DHCP snooping table
  - Drops the altered frames with incorrect MAC addresses
  - Allows the frames with correct MAC addresses
- Is used to prevent ARP spoofing attacks



Several types of attacks like Man-in-the-Middle (MITM) are conducted by poisoning the ARP cache. To prevent such attacks from taking place, you need to use the dynamic ARP inspection. To use the dynamic ARP inspection, you need first to enable the DHCP snooping feature, which is a pre-requisite.

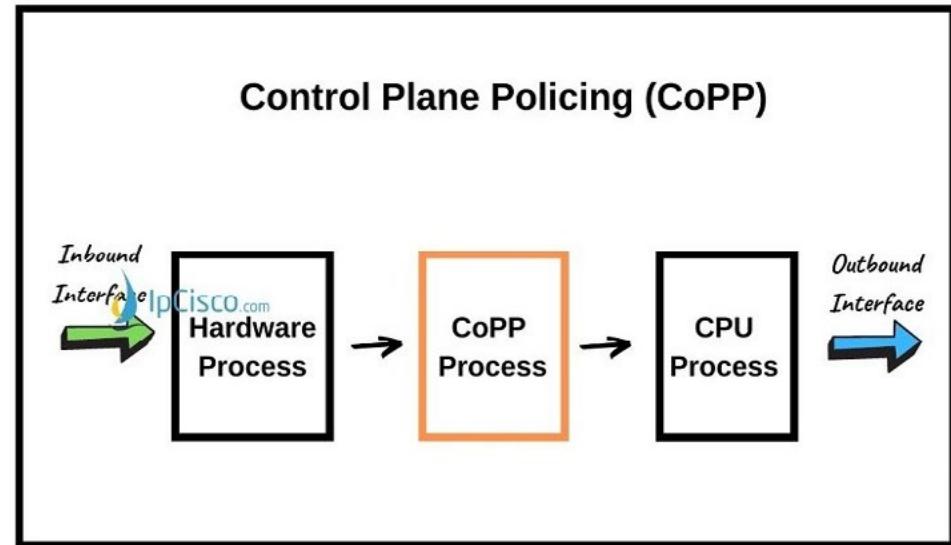
With the use of the DHCP snooping feature, it performs the IP address-to-MAC address mapping to ensure that the frames have the correct MAC address. If the switch locates any frame with a modified or changed MAC address, it drops the frame and does not forward it to the destination. If the frames are carrying the correct, they are forwarded to the destination.

When the dynamic ARP inspection feature is used, it defines a trust state for each port on a switch. The dynamic ARP inspection takes place on the ports that are marked as untrusted. The ARP traffic is examined on these ports.

Spoofing attacks can also occur if the dynamic ARP inspection is not enabled, along with the MITM attack. When this feature is enabled, it drops the spoofed packets.

# Control Plane Policing

- Is used to protect the control plane from network attacks
- Is policing the traffic to the control plane by:
  - traffic classification
  - Queue mapping
  - Queue shaping
- Applies the Quality of Service (QoS) policy on the control plane of the router
- Prevents Denial-of-Service (DoS) attack



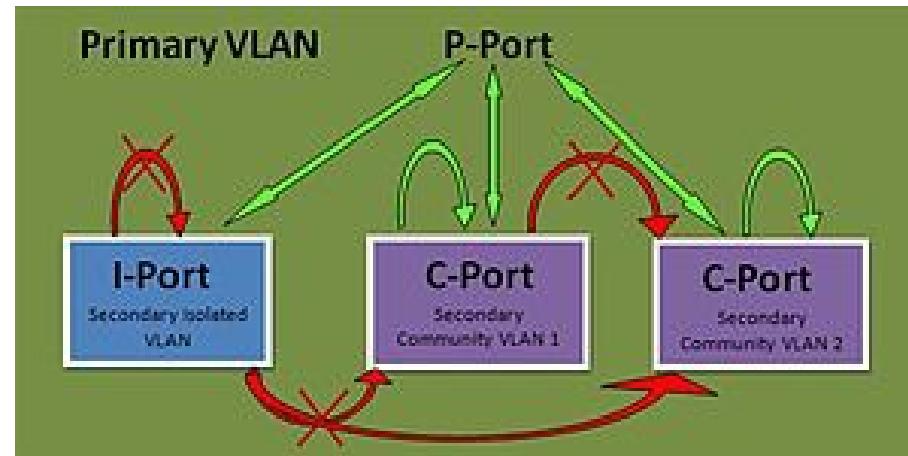
When you have a network, its architecture consists of three different planes: control plane, data plane, and management plane. The control plane is responsible for carrying the routing traffic to the router. The data plane carries the user traffic. The management plane is used for administering the routers.

Control plane policing is used to protect the control plane from any network attack, such as DoS attacks. The key intent of the control plane policing is to control the traffic that arrives at the router. This is done by using traffic classification, queue mapping, and queue shaping.

Quality of Service (QoS) policy is used to limit the traffic that arrives at the router. This policy is applied to the control plane on the router. It ensures that the router is not overwhelmed by traffic, and therefore, the traffic is classified and queued in different traffic queues, which are processed using the round-robin method. Each queue also has a limit to ensure that the router is not overloaded.

# Private VLANs

- Is the VLAN that is part of the main VLAN
- Is also known as port isolation
- Breaks the Layer 2 broadcast domain into several small subdomains
- Contains:
  - Several private ports
  - One uplink



A Layer 3 switch can be divided into several VLANs. Based on the configuration, these VLANs talk to each other, and routing is then configured to allow the traffic from one VLAN to another. You have the main VLAN, which can contain several secondary VLANs, considered private VLANs. The secondary VLANs are of two types:

- Community: contains devices that communicate with each other
- Isolated: contains devices that cannot communicate with each other but to the switch only

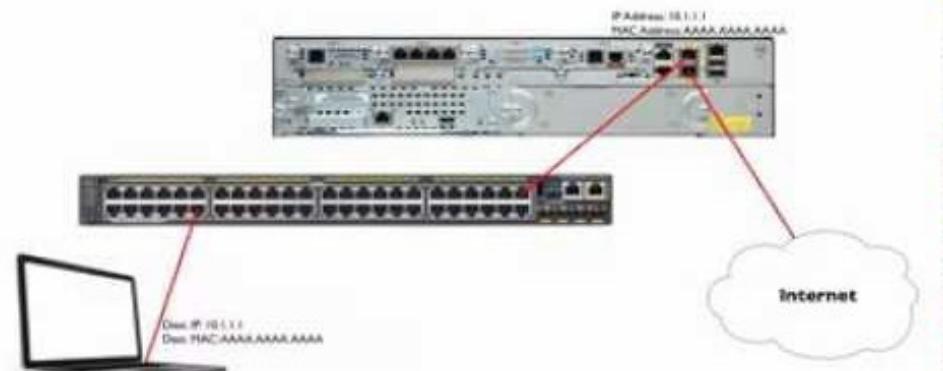
You have the broadcast domain at Layer 2. With the use of the private VLAN, each broadcast domain is broken into smaller subdomains. Within each subdomain, you can have a primary VLAN and several private VLANs.

The private VLAN is the isolated VLAN that allows the devices to communicate with the switch that has an uplink configured. This method is also known as private VLAN. Within a VLAN, you can configure several ports, but you can have only one uplink.

# Disable Unneeded Switchports

- Prevents a malicious entity to plug-in a device into a wall outlet port
- Prevents unauthorized devices to be live on the network from an unused port
- Prevents attacks like:
  - MAC flood attack
  - Denial-of-service attack
  - Traffic sniffing

## Shut Down Unused Ports



Most switches have 24 ports that are connected to the wall outlets where users plug in their systems. Anyone can connect a system to the wall outlet and use this port. There can be a possibility that one of the switch ports is lying idle even though it is connected to a wall outlet. This often happens when you have visitors who conveniently connect their systems to these wall outlets.

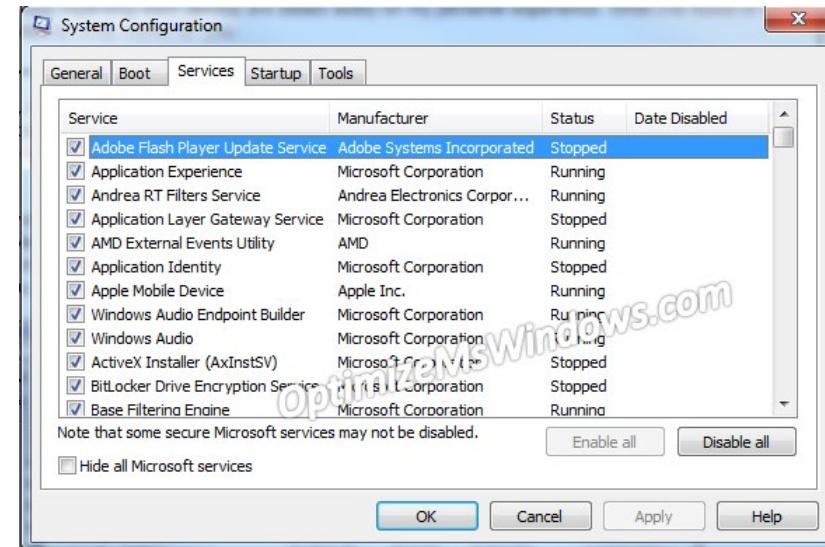
If a wall outlet is not being used, you should simply disable the switch port. This will prevent any malicious entity from plug-in a device, and it will also prevent several incidents, such as:

- MAC flood attack
- Denial-of-Service attack
- Traffic sniffing

Anyone plugged into an unused port becomes a part of the network and can launch any of these attacks. Therefore, it is better to disable the unused ports.

# Disable Unneeded Network Services

- Requires any unwanted service to be stopped to prevent it from being exploited
- Can be determined by running the netstat -a command
- Requires shut down of ports that is linked with the unnecessary service



When you install a system, it has several services that are running. Some of the services are used by the operating system, and some are running to provide extra services, which you may or may not need. Each service that is running requires a port to be opened. For example, if you run an FTP server on your system, you are opening port 21. Whenever a user connects to the FTP server, they are connecting to port 21. A normal user would not go beyond this point. However, a malicious user would use the port to get into your system. Therefore, you need to ensure that you shut down all the services that are not required. This way, you are reducing the attack surface in your system.

You can use the Services console in Windows to determine the running services. However, a quicker way is to use the netstat -a command. It will show you the services and ports that are being used in real-time. If you shut down the port, it will prevent anyone from accessing its related service on your system.

It is important to note that the more services you run, the more vulnerable you become. Keeping this in mind, you should shut down all unnecessary services.

# Change Default Passwords

- Default passwords:
  - Are configured in almost all networking devices
  - Are used to provide initial access to the user
  - Can lead to several attacks, such as loss of device control or unwanted configuration changes
  - Should be changed immediately as soon as device is powered on
  - Is mentioned on the device's documentation or can be researched from the Internet



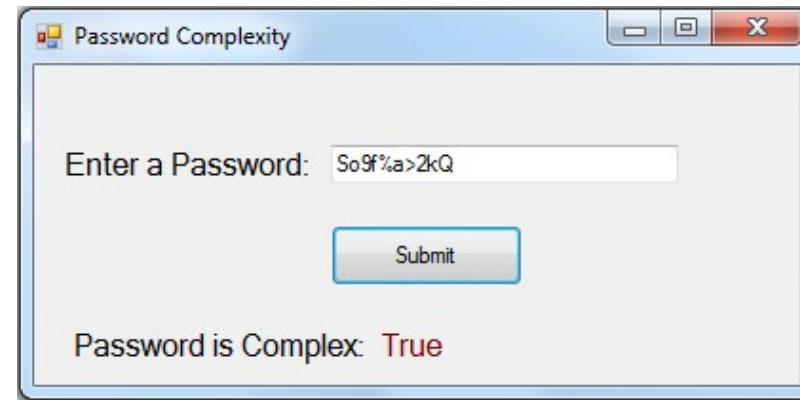
Network devices, such as routers, wireless routers, and switches, come with the default configuration. A username, such as admin or administrator, and a password are part of the default configuration. With the default credentials, the username, and password, an administrator can configure the networking device. However, as a security practice, the default password and preferably the username should be changed on the network device after the initial configuration.

If the default credentials are not changed, then there can be several security issues. For example, if the device is lost, whoever finds it can try the default credentials to gain access. Also, if the device is live on the network, someone can simply change the configuration. Therefore, changing the default credentials is a must on all these devices.

It is not hard for someone to find the default configuration. Many websites provide the default username and password for networking devices. These websites do not list these default credentials for any wrong purpose but to help users find the default credentials. For example, if you have reset a wireless router and don't know the default credentials, you can search it on the Internet.

# Password Complexity/Length

- Makes a password complex to prevent an easy password cracking
- Should be at least 8 characters in length
- Should be a mix of:
  - Upper and lowercase letters
  - Numbers
  - Special characters
- Does not use dictionary words or names



Most users are used to keeping an easy password. For example, if you search on the Internet, the passwords like password and 123456 are still the most widely used. If you use a password cracker, these passwords can be cracked in one second.

If you have ever attended a cyber security training, one of the key messages from the training is to use a complex password. The reason behind using a complex password is that it will make it difficult for the attacker to crack the password. With the complex password, if you make it 8 to 15 characters long, it serves the purpose because cracking a long, complex password will take years.

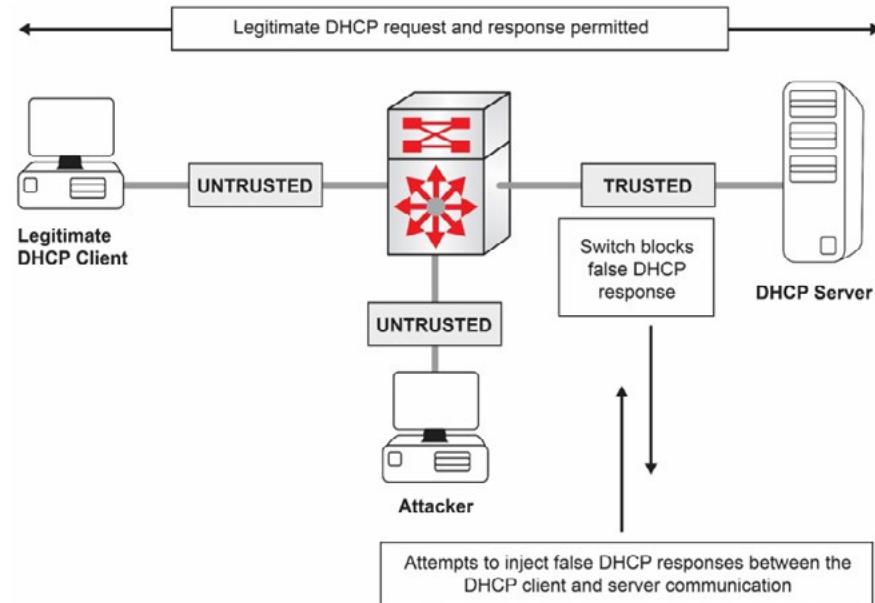
So, the question is what comprises a complex password. It should include:

- Upper and lowercase letters
- Numbers
- Special characters

Most users prefer to avoid using a complex password as it can be hard to remember. So, as an easy way out, these users make a lengthy password, such as RogerMoore. Even though this password has 10 characters, but it can still be cracked in a few minutes. As one of the key guidelines for passwords, you should avoid using dictionary words or names. For example, RogerMoore should not be used as a password. Sunflower is a dictionary word. You should avoid using such words and names.

# Enable DHCP Snooping

- Is a switch feature that prevents the network devices to communicate with the unauthorized DHCP
- Have the trusted ports on which the DHCP server are connected
  - Clients accept requests only from these DHCP server
  - Rogue DHCP servers cannot respond to the client requests



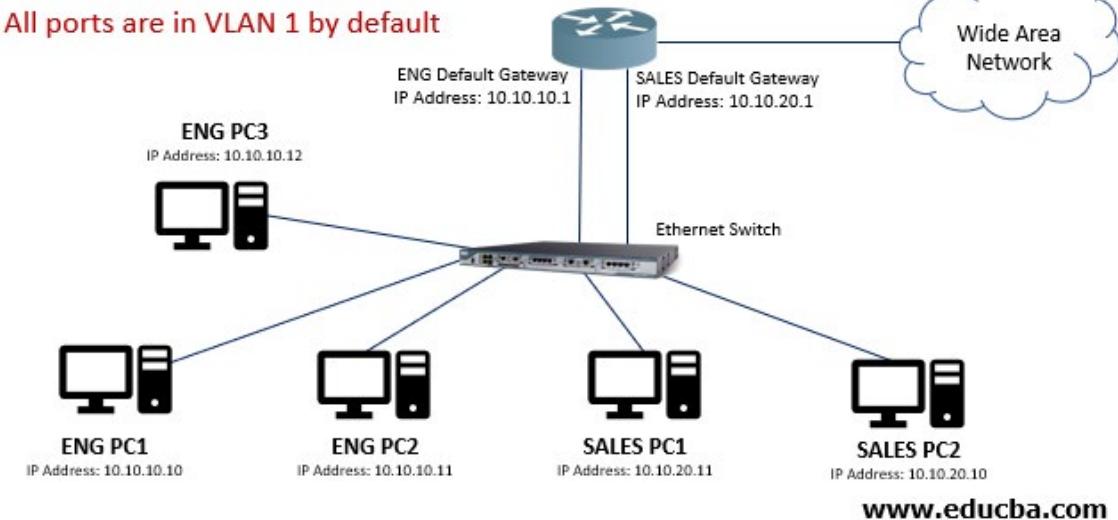
You learned about the rogue DHCP in the previous lesson, which can lease IP addresses to networked clients. To prevent a rogue DHCP from existing on the network and leasing IP addresses, you should use the DHCP snooping feature, which is provided in the switches. When you enable this feature in a switch, it prevents the network devices from communicating with the unauthorized or rogue DHCP.

You have to define the trusted ports and plug the DHCP servers on to these ports on a switch. When you do this, the DHCP servers on these ports can cater to the client's requests. The unauthorized or rogue DHCP server cannot respond to these requests.

The switches also have a binding table that contains the IP address-to-MAC mappings. Any packet that arrives at the switch and does not match the bindings in the table is dropped.

# Change Default VLAN

- Default VLAN
  - Is the VLAN1 in switches
  - Is the VLAN on which all switch ports are assigned by default
  - Cannot be deleted or modified
  - Is a target of attack
- Is the method of creating another VLAN and assigning switch ports to it



Switches follow the concept of VLAN and have VLAN1 as the default one. The VLAN1, by default, contains all the ports available on the switch. It remains as is even if it does not contain any port. Unlike the other VLANs you create on a switch, you cannot modify or delete the VLAN1.

The VLAN1 is the default VLAN that is used for control plane traffic. However, it can also be used for the user traffic as well. Because VLAN1 exists on all switches and cannot be changed or renamed, it becomes the target of attacks.

It is always recommended that the user traffic be moved to another VLAN to prevent unnecessary broadcast traffic. To do this, you need to create another VLAN and move the ports to the new VLAN.

# Patch and Firmware Management

- Is used to update patches and updates to the devices, applications, and operating system
- Is driven by patch management policy
- Can be configured as an ongoing automated task
- Is used to:
  - Patch up the vulnerabilities or security flaws
  - Add a new feature
  - Resolve a technical issue



There can be vulnerabilities in software, or there can be an enhancement. From time to time, the software companies release patches and updates for applications, operating systems, and even firmware embedded into the devices or systems. Most organizations follow a patch management policy through which they roll out the updates and patches.

For example, a Windows update is released. Depending on its criticality, it might be immediately rolled out or rolled out a few days later, along with the other updates. The patch management policy should drive this.

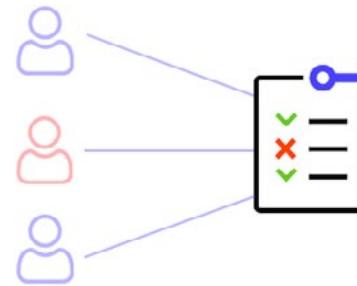
Several organizations have the patch management applications, such as Windows Software Update Service (WSUS), to roll out the patches automatically. However, the patches are first tested in most cases and then approved for rollout. After the patch is rolled out, it can be tracked in terms of how many systems have this patch and pending.

It is not always that the patches are released to fix a bug or vulnerability. It could be due to other reasons, such as adding a new feature or resolving a technical issue. It could be that there is an update on the device driver.

# Access Control List

- Allows or denies access to users on network resources
- Can be of two types:
  - Filesystem
  - Network
- Can be used to:
  - Filter network traffic
  - Network restrictions
  - Files and folder restrictions

## Access Control List



You attempt to access a shared folder on your office network, but you are prompted with an access denied message. The network administrator or the shared folder owner has used the access control lists or ACLs to deny you access to the shared folder. This is what the ACLs are used for – they allow or deny access to the users on a network or an operating system resource. For example, when you share a folder, you can allow certain users and deny access to the remaining. You are practicing the use of ACLs in this scenario. You can either allow or deny access to the users on a specific resource.

ACLs are of two types:

Filesystem ACLs: are applied on the operating system components, such as files and folders, to allow or deny access to the users

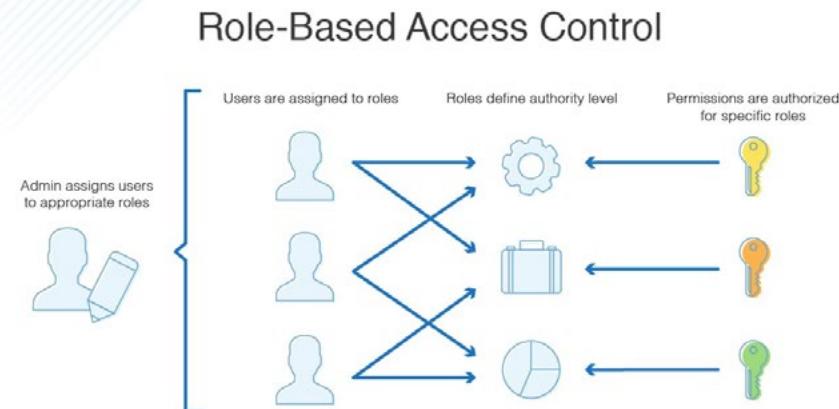
Network ACLs: are applied on the network components, such as routers and switches, to filter the traffic

There are various use cases for ACLs. They can be used to:

- Filter traffic over the network – allow or block traffic into and out of a network
- Restricted network access – restrictions on the traffic flowing between subnets
- Network restrictions - restrictions to shared folders and files
- Operating system files and folders – restrictions to folders and files

# Role-based Access

- Is assigned to a user who is performing a specific job role
- Is delivered to the user by using the security groups
  - Users have a specific role
  - Roles define the security groups
  - Permissions are assigned to the security groups
- Can allow a user to have several roles



Most organizations have role-specific security groups. Before understanding role-based access, it is important to understand that a security group is a collection of users to which the permissions can be assigned on a network resource. Let's take an example of a security group named Accounts that has several users. You can assign permissions to the Accounts group on a network folder, and all users within the Accounts group are granted permissions.

So, within the organizations, several security groups can be created based on the job roles, such as Accounts, Finance, Senior\_Management, etc. The users who are in those job roles can be added to these groups. Whenever permission needs to be assigned to a specific job role, all you need to do is assign permissions to the security group, and all users within the group inherit permission.

From the ease of administration, it is good to use the security groups. For example, if you need to remove users with a specific job role from a shared folder, all you need to do is remove the group, and users in that group lose their permissions on the shared folder. Imagine if you had to do this for 100 users individually. It would have taken a much longer time.

It is also important to note that a user can belong to several groups. For example, James can be in the Senior\_Management group as well as the Accounts group. There is no limitation to the number of groups a user can be added to.

# Firewall Rules

- Control the inflow and outflow of the network traffic from a network
- Can control the traffic:
  - To be allowed
  - To be blocked
- Can use the following:
  - Explicit Deny – known as blacklisting – all traffic allowed except the one that is specifically denied
  - Implicit Deny – known as whitelisting - all traffic is denied except the one that is specifically allowed

The screenshot shows a software interface titled "SmartConsole" with a tab for "Firewall". The main window is titled "Policy" and displays a table of rules. The columns include No., Hits, Name, Source, Destination, VPN, Service, Action, Track, Install On, and Time. The rules listed are:

No.	Hits	Name	Source	Destination	VPN	Service	Action	Track	Install On	Time
1	9K	Stealth	Corporate-inte	GW-group	Any Traffic	Any	drop	Alert	Policy Targets	Any
6	203K	Outbound HTTP	Remote-2-inter	Any	Any Traffic	TCP http	Client A	Log	Remote-2-gw	Any
7	3K	Critical subnet	Corporate-inte	Corporate-rn	Any Traffic	Any	accept	Log	Corporate-gw	Any
8	101K	Tech support	Tech-Support	Remote-1-web-	Any Traffic	TCP http	accept	Alert	Remote-1-gw	Any

A firewall is used for filtering the ingress and egress traffic – this means the incoming and outgoing traffic from a network. The traffic filtering is performed based on rules that you define. For example, a firewall rule blocks the outgoing FTP traffic, and another rule blocks the incoming FTP traffic.

When you define a firewall rule, you either allow the traffic or block the traffic. In most cases, the traffic rules are defined based on the port numbers. For example, if you need to block the outgoing FTP traffic, you need to block the port number, and the FTP traffic will be blocked. Usually, the last rule blocks all the traffic that is not allowed using the permit statements.

You would typically define two types of rules:

- Explicit Deny – known as blacklisting – allows all traffic unless explicitly denied. For example, if you have a rule blocking FTP traffic, all other traffic will be allowed.
- Implicit Deny – known as whitelisting - blocks all traffic unless explicitly allowed. For example, FTP is allowed, but the rest of the traffic is blocked.



## *TOPIC 2*

---

# WIRELESS SECURITY

---

# MAC Filtering

- Restricts the wireless devices to connect to the wireless routers or access points
- Adds the MAC address of the allowed devices into the whitelist
- Denies access to the devices whose MAC addresses are not allowed

Add or Modify Wireless MAC Address Filtering entry

MAC Address:	00-19-66-CA-8B-C7
Description:	Wireless MAC Filter One
Status:	Enabled

Save      Back

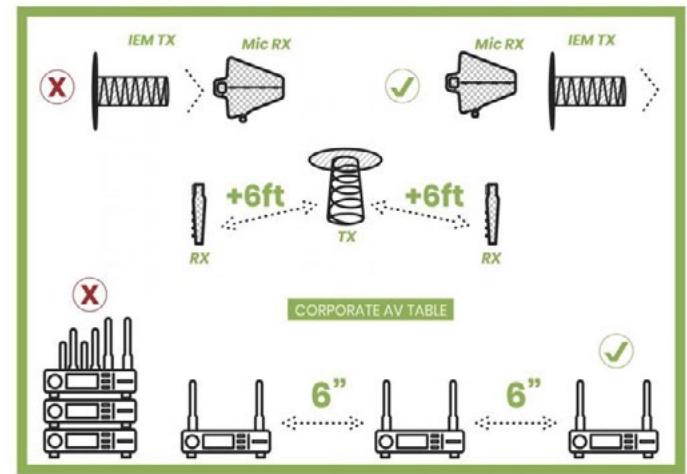
Let's say that you have a wireless network at home. You know the password and add several devices. This means that anyone who knows the password can connect a device to your wireless network. To prevent this from happening, you can enable a feature called MAC filtering. When you enable MAC filtering, you can add the MAC addresses of the known devices in the whitelist. This means that if a device's MAC address is added to the whitelist, it will be allowed to connect to the wireless network. The rest of the devices whose MAC addresses are not in the whitelist will be denied access.

Even though this is a security method, it can be bypassed by using a spoofed MAC address. However, at home or in small offices, this method serves its purpose.

# Antenna Placement

- Need to be decided after the site survey
- Should be strategically placed so that there is minimum interference
- Should ideally be placed in the middle of the location where users are placed
- Should consider the exposed signals while placing the antenna

## Antenna Placements Examples



Stephen Pavlik

sounddesignlive.com

Before setting up a wireless network, you should perform a site survey, which helps you decide where the wireless routers or the access points need to be placed. Whenever you are placing them, you need to ensure minimum interference from the other devices. For example, you do not want to put the wireless router or the access point close to walls or objects that block the signals. You need to put it in a place where the signals can be broadcast in all directions.

For example, if it is a room where 50 people are sitting, putting the wireless router in a corner will not help. You should place it in the middle of the room to broadcast the signals in all directions.

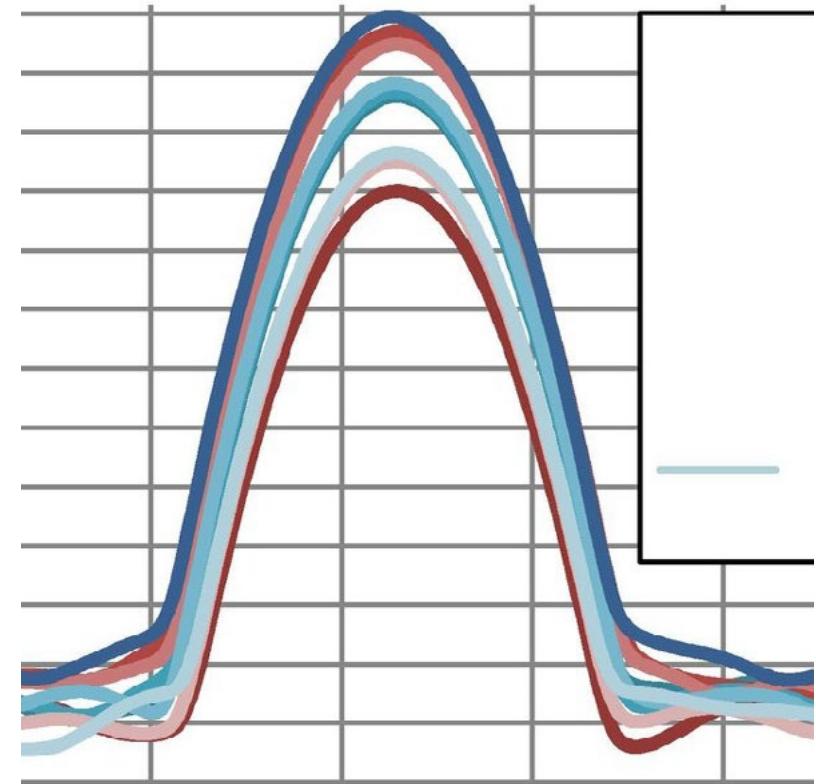
Other than the wireless router or access point placement, the correct type of antennas should be used. You should strategically place the wireless antenna so that it can broadcast the signals in all directions. The wireless routers and access points have Omni-directional antennas, which transmit signals in all directions equally.

The key advantage of Omni-directional antennas is that they are easy to install. You can place them in any direction or location in a room. You will still get the signals in all corners of the room.

The key disadvantage of Omni-directional antennas is that they have a shorter range as they transmit the signals in all directions. Since the signals are spread out, they reach only a certain distance.

# Power Levels

- Should strategically place to ensure optimum signals are broadcast to surrounding locations
- Should not broadcast signals outside the building
- Should be at the apt level for the users

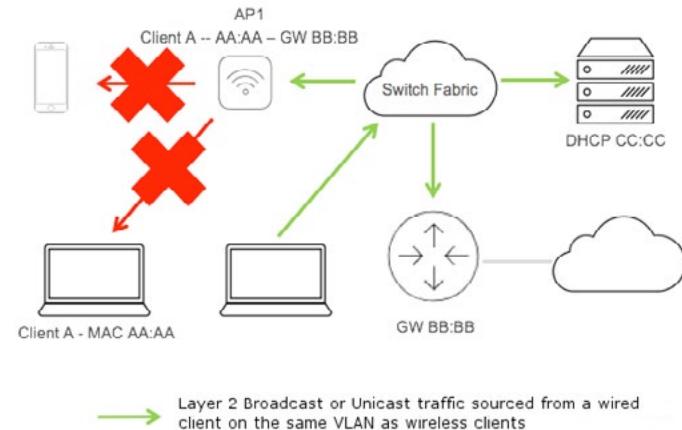


The wireless network administrators try to place the wireless router or access point so that the signals can reach all corners of the office. It is good to do that because every wireless client gets a decent amount of wireless signals. However, this poses a security threat – the signals can reach outside the building – maybe into the parking lot.

The wireless signals can go out of the building if the wireless router or access point is not placed properly. For example, if you have installed the wireless router on a wall that is the edge wall of the building, then it is obvious that the signals will be broadcasted outside. To handle this situation, you need to change the location of the wireless router. The location should be somewhere in the middle of a room so that everyone gets the optimal level of signals. When you do this, the chances of signals going outside the building reduce.

# Wireless Client Isolation

- Isolates a wireless client from the remaining ones
- Prevents communication from the isolated client to the rest of the clients
- Allows only the Internet access to the isolated client
- Prevents communication with the wired network

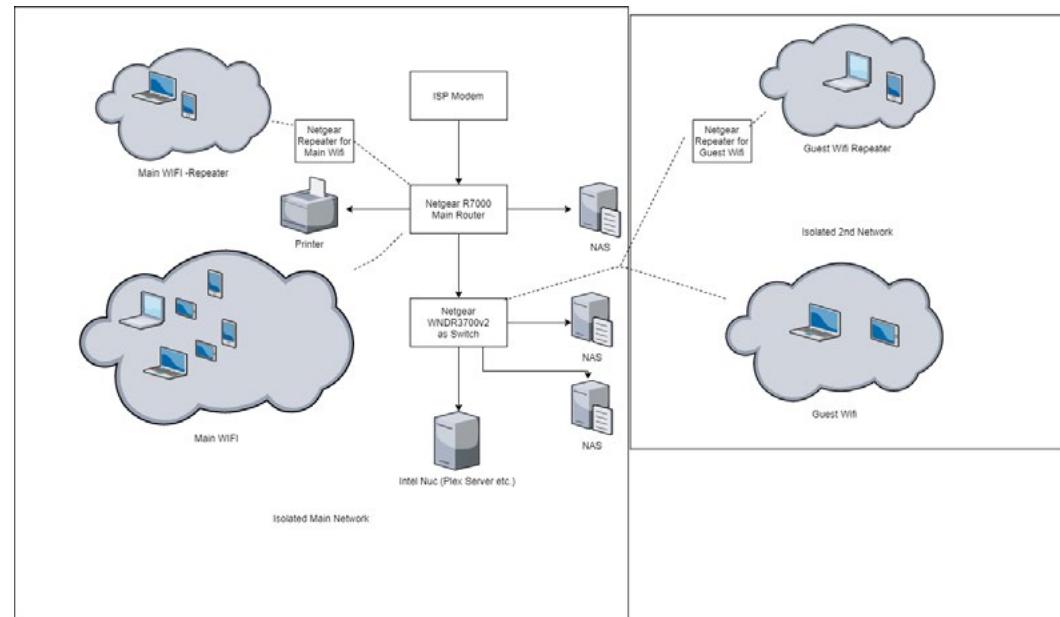


Wireless Client Isolation is a feature that allows you to isolate wireless clients from the main wireless network. Assume that you have several clients on a wireless network. If one device needs to connect, but you do not want it to have full access to the wireless network, you can enable the Wireless Client Isolation feature.

Even though the device will be able to connect to the wireless network, it will not communicate with the other clients. The device will only connect to the Internet via the wireless network but not perform any other communication. This also prevents the device from accessing the wired network to which the wireless network is connected.

# Guest Network Isolation

- Creates a separate network for the guests
- Keeps the guest network separate from the production wireless network
- Has limited access – only the Internet access

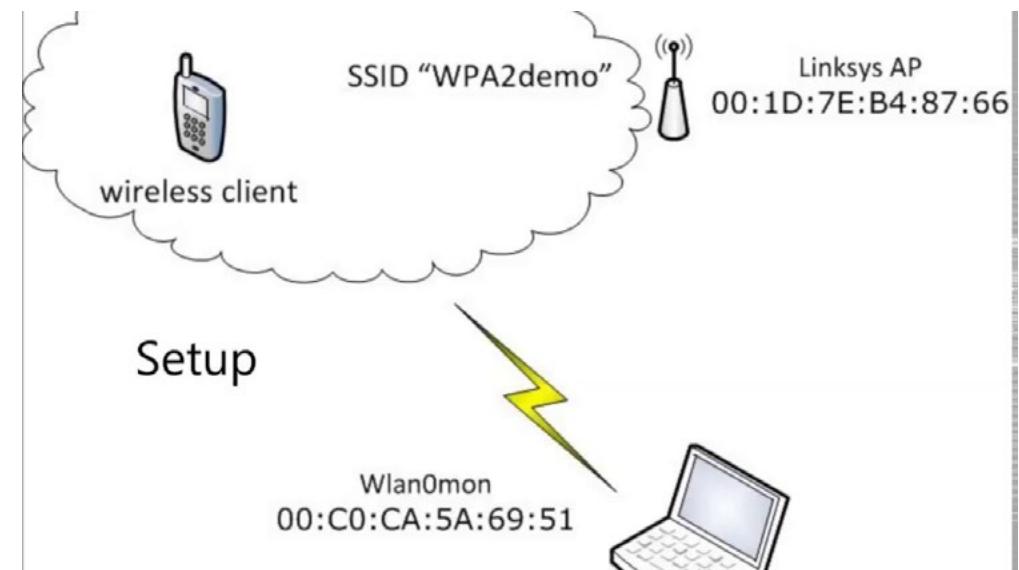


Most wireless routers can configure a guest wireless network. If you allow visitors to connect to the main wireless network, they have access to the entire wireless network. They can also connect to the wired network through the wireless network. Therefore, it is better to segregate their network to have limited access, which can be achieved with the guest network. For example, you can allow only Internet access on the guest wireless network.

When a device connects to the guest wireless network, it cannot communicate with the main wireless network. Both wireless networks are separate.

# Preshared Keys (PSKs)

- Is a client authentication method on wireless network
- Is usually used in smaller wireless networks
- Uses Temporal Key Integrity Protocol (TKIP) to generate encryption key
- Are same with the client and wireless access points

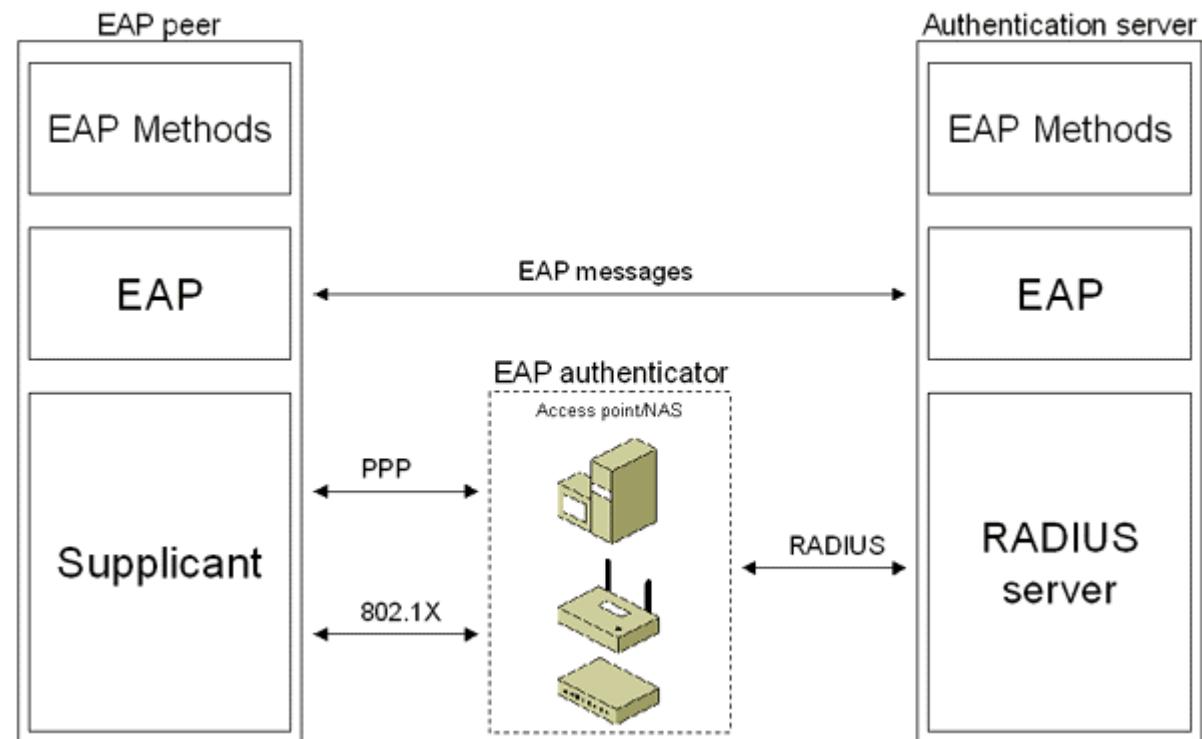


The smaller wireless networks use the Preshared Keys (PSKs) method as one of the client authentication methods. On the other hand, the larger wireless networks use the enterprise method that requires a RADIUS server. In the PSK method, the Temporal Key Integrity Protocol (TKIP) method generates the encryption key, which is a 64 hexadecimal digits string.

The clients and the wireless router or the access points have the same PSK that is changed regularly. When both the clients and the wireless router or access point have the same PSK, the users need to provide the password to connect to the wireless network.

# EAP

- Is used by 802.1x to carry the authentication information
  - Does not secure the authentication information
- Is used with WPA2 and other wireless protocols
- Has variants
  - Some variants use certificates
  - Some variants use passwords

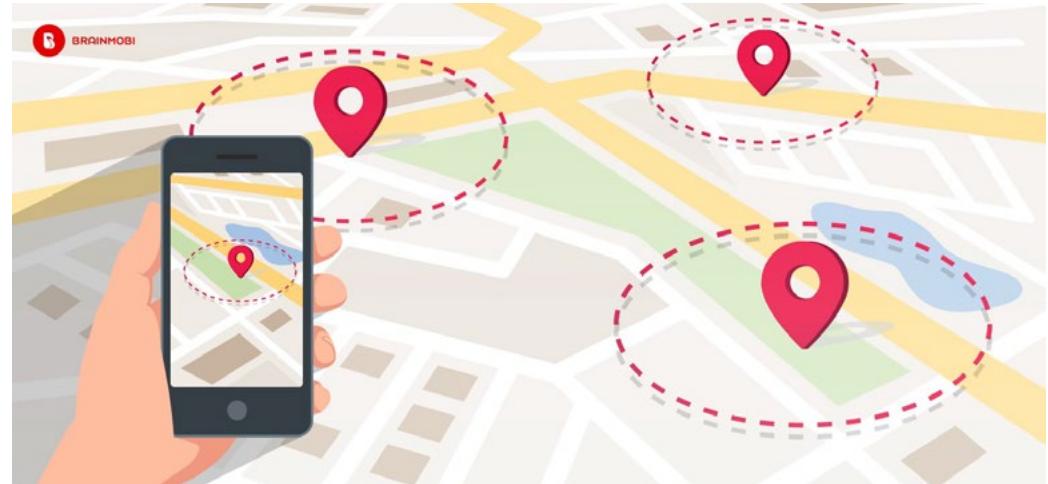


EAP stands for Extensible Authentication Protocol, which is used with the 802.1x to carry the authentication information. EAP is not an authentication method but rather a framework that includes EAP methods used for authentication negotiation. Since it is not an authentication method, it does not secure the authentication information. It carries the information in its original format. It is mainly used with the WPA and WPA2 wireless standards.

EAP has several variants where it is used. Some of the key variants are Lightweight Extensible Authentication Protocol (LEAP), EAP Transport Layer Security (EAP-TLS), EAP Pre-Shared Key (EAP-PSK), and EAP Flexible Authentication via Secure Tunneling (EAP-FAST). Some of the variants use certificates for authentication, while others use passwords.

# Geofencing

- Defines a perimeter for the mobile devices
  - If the device moves out of the perimeter, an alert is generated
  - It can also send promotional messages based on a device's location
- Uses Global Positioning System (GPS) or Radio Frequency Identification (RFID)



Using the geofencing method, you can define a perimeter for the mobile devices. For example, you have a mobile device, such as a tablet, that should always be in the office, and no one should take it out. You can use the geofencing method to define a perimeter for the tablet. If anyone attempts to take the tablet out of the office, the administrator can generate an alert.

Geofencing is also being used for promotional services. For example, have you ever received a notification or SMS about a product when you entered a shopping mall? This happens quite often. As soon as you enter a shopping mall, you start to receive promotional SMS. The location-based service (LBS) is used to track whether the user has entered a defined perimeter.

The geofencing method can work using either of the following methods:

- Global Positioning System (GPS)
- Radio Frequency Identification (RFID)

# Captive Portal

- Is an authentication mechanism used with wireless network
- Is the first webpage that users gets to see when they initiate a connection to the wireless network
- Requires the user to first authenticate using a portal
- Can also display an Acceptable Use Policy (AUP) that user has to accept to get access

**Example Captive Portal**

Welcome!  
Please enter your credentials to connect.

Username:

Password:

Access Code:

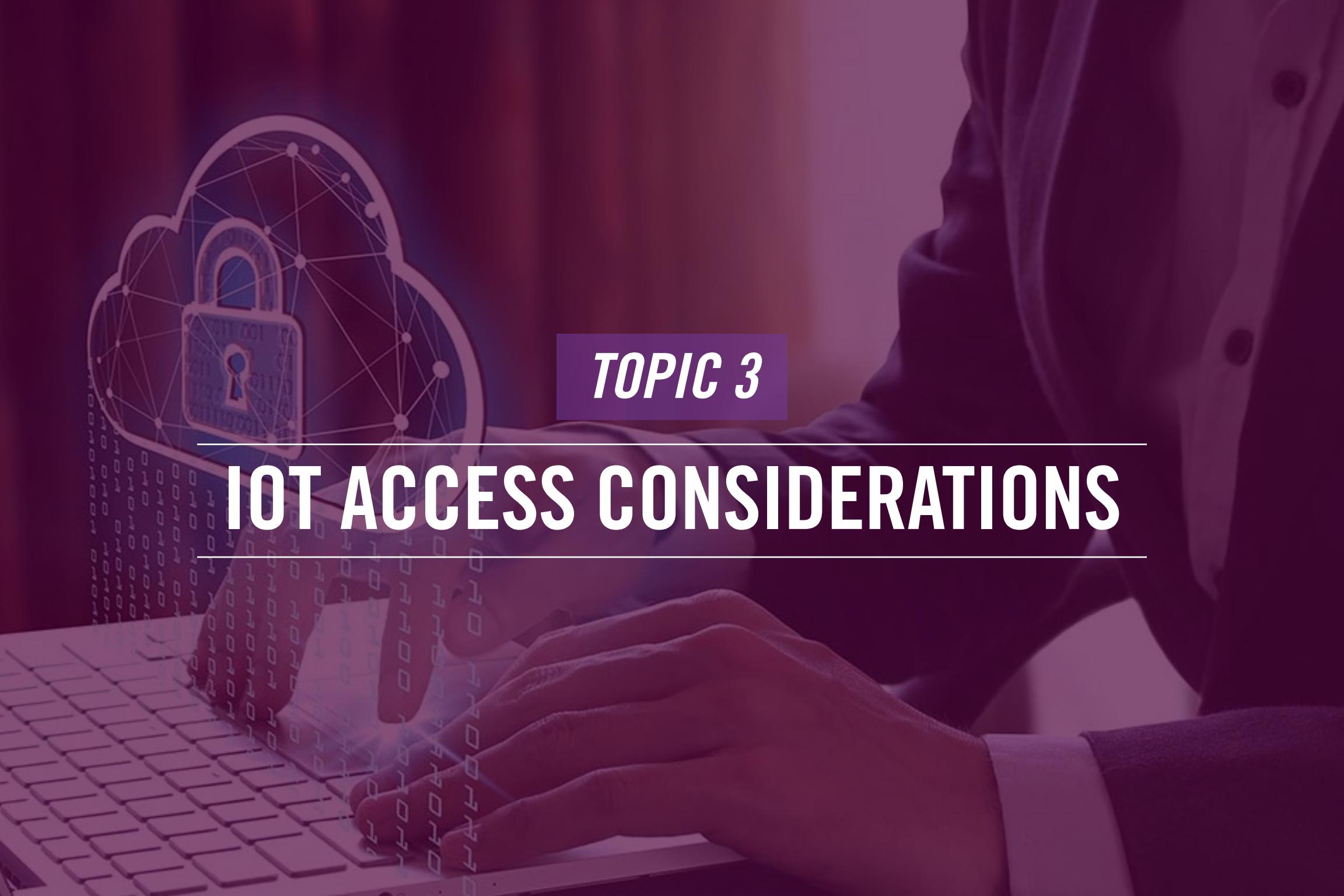
Terms and Conditions

1. The owner and operator ("Owner") of this computer network ("the Service") reserves the right to discontinue the Service at any time.

I agree to the Terms and Conditions

Hotels, airports, and cafes generally provide free wireless connectivity. To be able to use the free wireless network, they provide the login details. However, to use that login details, you need to connect to a portal and feed the login information. The portal you connect to is the captive portal, an authentication mechanism used with wireless networks.

When you connect to the wireless network, you are firstly redirected to a webpage that asks for the login credentials. In some cases, it also requires you to feed the mobile number to which the SMS with an OTP can be sent. After you feed the OTP and accept the acceptable use policy, you can use the wireless network.



## *TOPIC 3*

---

# IOT ACCESS CONSIDERATIONS

---

# IoT Access Considerations

- Use the secure DTLS protocol
- Use Public key cryptography
- Create a separate IoT network
- Implement controls for spoof protection
  - Each IoT device should have unique identity
- Update all software



IoT devices are considered to be insecure. When the concept of IoT was inception, security was not considered a prime factor. It was only the communication that had to be performed by the IoT devices by sending their data to a central entity. Due to this, IoT devices are being targeted in various security attacks. For example, IoT devices, after they are compromised, are being used as bots or zombies to conduct a DDoS attack.

The IoT communication is also not secured by default. To secure the communication from eavesdropping or man-in-the-middle attacks, you can implement the Datagram Transport Layer Security (DTLS) protocol, which works on the UDP protocol to encrypt the communication.

You can also use Public Key Cryptography (KPI) to secure the communication using encryption.

Another method to enhance IoT security is to put them into a separate network, further protected by limiting their access.

You should also ensure that each IoT device has a unique identity not to be spoofed. The last method is to ensure that all IoT devices have updated firmware and patches. If there is a known vulnerability, it should be patched before an IoT device is put into the production environment.

# Summary

- Best Practices
- Wireless Security
- IoT Access Considerations



That's the end of the lesson.  
Here we covered:

- Best Practices
- Wireless Security
- IoT Access Considerations



A person with curly hair, wearing glasses and a headset, is sitting at a desk and looking down at a laptop screen while writing in a notebook.

*NEXT TOPIC*

---

## REMOTE ACCESS METHODS

---

Lesson

# 4

# Remote Access Methods

- 1 — Welcome to the 4 lesson of Module 4. In this lesson, you will learn about the:
- 2 — Remote Access Methods



Network Fundamentals

# Agenda

- Site-to-site VPN
- Client-to-site VPN
- Remote desktop connection
- Remote desktop gateway
- SSH
- Virtual Network Computing (VNC)
- Virtual Desktop
- Authentication and Authorization Considerations
- In-band vs. Out-of-band Management



Hi, welcome to COMPTIA Network+ Course

In this lesson, we will talk about:

- |  |   |
|--|---|
| <ul style="list-style-type: none"><li>• Site-to-site VPN</li><li>• Client-to-site VPN</li><li>• Remote desktop connection</li><li>• Remote desktop gateway</li><li>• SSH</li></ul> | <ul style="list-style-type: none"><li>• Virtual Network Computing (VNC)</li><li>• Virtual Desktop</li><li>• Authentication and Authorization Considerations</li><li>• In-band vs Out-of-band Management</li></ul> |
|--|---|

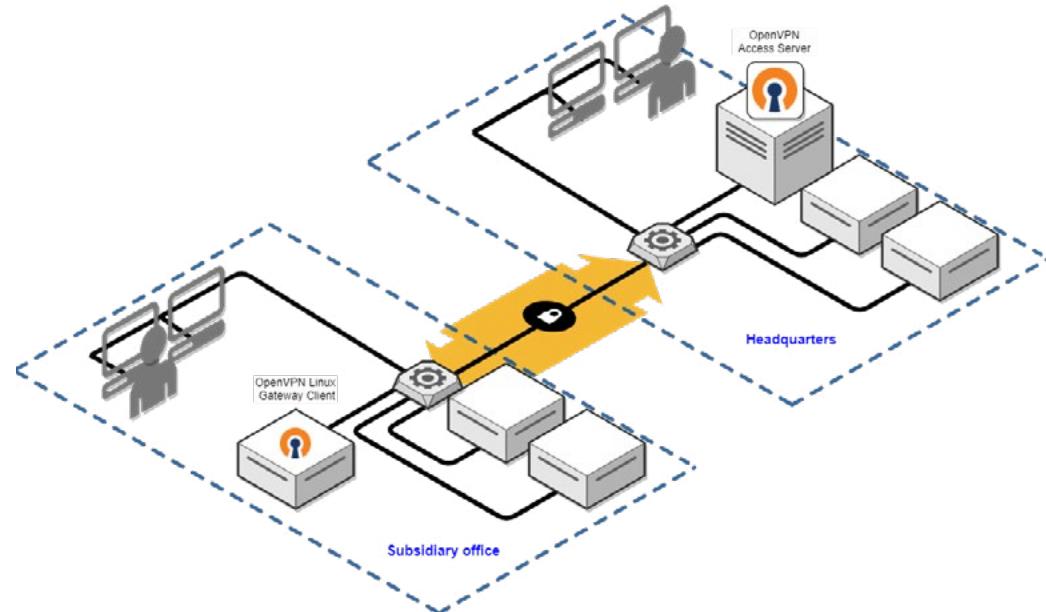


## *TOPIC 1*

# SITE-TO-SITE VPN

# Site-to-site VPN

- Connects two different sites over the Internet connection
- Removes the dependence on the WAN connections, such as Frame Relay
- Create an encrypted channel between two sites to share data
- Can be set up between two or more networks
  - Can be one to many sites
  - Can be many to many sites



Site-to-site VPNs are VPN connections between two sites. They are usually established between two edge routers or VPN devices. You can establish a site-to-site VPN connection between:

- A remote branch site and main office
- Two organizations who need to share information

For example, organizations can use the VPN connection that allows them to share files rather than putting up an FTP server to share files over a secure channel. This method can work between a branch and corporate office and between two or more organizations. Therefore, you don't rely on a WAN connection to be present on the Internet to share files. You can remove the dependence on WAN connections, such as Frame Relay or any other Internet-based protocol.

When a VPN connection is established, all data is routed through the secure VPN tunnel. The VPN connection encrypts the tunnel, which helps the organization maintain the confidentiality of the data.

You can connect site-to-site VPN connections between one-to-many networks. For example, one organization can have several VPN connections with the branch office or partner organizations. On the other hand, there can be many-to-many site VPN connections. Each site has several VPN connections, such as SiteA has a VPN connection with SiteB and SiteC. On the other hand, SiteB has a VPN connection with SiteA and SiteB.



**TOPIC 2**

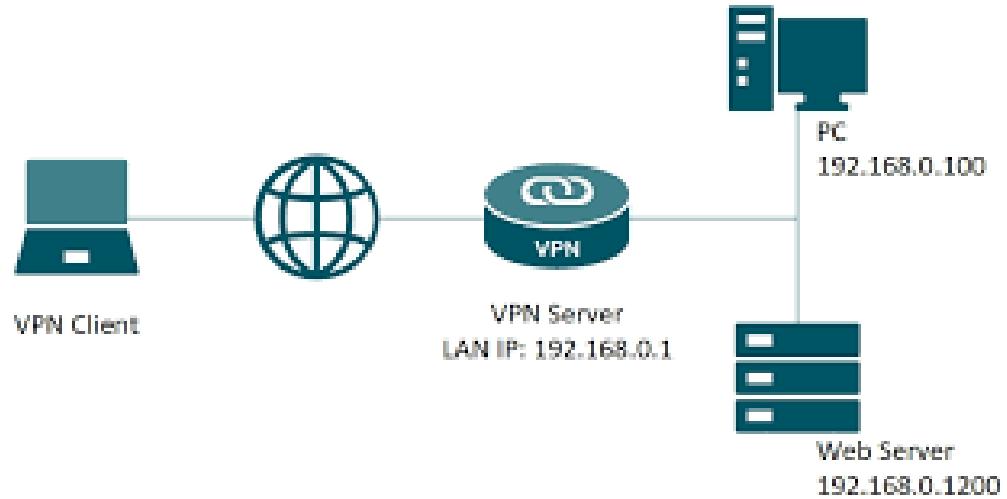
---

# CLIENT-TO-SITE VPN

---

# Client-to-site VPN

- Allows the users to remotely connect to the corporate network
- Works on demand – as and when and from wherever users want to connect
- Is usually done via a VPN client
- Allows the client to access network resources based on the permissions
- Can be configured as:
  - Clientless VPN
  - Split and Full Tunnel



In the site-to-site VPN connection, you learned that two sites connect using a VPN connection. On the other hand, the users connect to a VPN server with a corporate network within an organization with the client-to-site VPN connection. There are mobile forces, such as Sales and Marketing teams, that are always on the move. They need to connect back to the corporate network for various reasons. This type of VPN connection works well for them. With the client-to-site VPN connection, the users can connect to the corporate network as and when and from wherever they want to connect. They can move around and as and when required and use the VPN client to connect to the server in the corporate network. The clients usually work with the VPN client, which can create a profile for the user. By default, the user's profile is used to connect to the VPN server. The user's profile contains the user credentials and the VPN server name or IP address.

When a client connects to the VPN server, access to the network resources is granted based on the user's permissions. For example, a user can connect to only one specific folder on a file server.

The client-to-site VPN can be configured as a clientless VPN in which the client application is not used. The user can use the HTTPS-enabled Web browser to connect to the VPN server.

There are also split and full tunnels. In the split tunnel, the user connects to the VPN server and access the network resources. At the same time, the user can use the Internet connection that is pre-configured through a proxy or direct connection to the Internet. In the full tunnel mode, the user can only connect to the VPN server, and even the Internet connection is then routed through the VPN tunnel.

## *TOPIC 3*

---

# REMOTE DESKTOP CONNECTION

---

# Remote Desktop Connection

- Is available in Windows by default
- Allows you to remotely connect and control the system
- Uses the Remote Desktop Protocol
- Provides the graphical interface rather than a terminal window like SSH
- Uses Port 3389



Remote Desktop Connection is available as a remote connectivity tool in all recent versions of Windows. With this tool, you can connect to a remote Windows server or system and control it like you are physically working on the system. However, this works except you have the permissions to connect to the remote system. For example, if you need to manage a server remotely, you must assign yourself the permissions to use Remote Desktop Connection. This is typically done through Group Policy, and if it is a standalone system, you need to add yourself to the Remote Desktop Users group on this system.

The Remote Desktop Connection tool uses the Remote Desktop Protocol, a Microsoft-proprietary protocol. It creates an encrypted connection with the remote system.

Other than this, if you are used to using SSH, which gives you access to the remote terminal shell, Remote Desktop Connection provides access to the graphical shell. You get to see the graphical mode of Windows like you do when you work on the physical system.

Remote Desktop Connection, as stated earlier, uses RDP that uses port 3389.

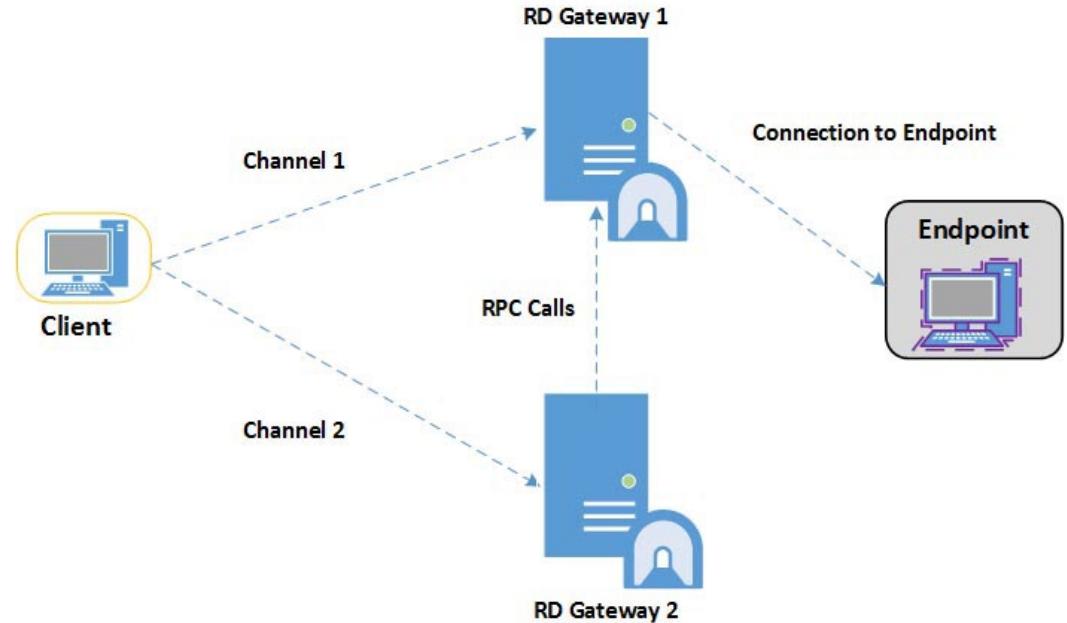
## TOPIC 4

# REMOTE DESKTOP GATEWAY



# Remote Desktop Gateway

- Is a Windows Server role
- Tunnels directly into the system using a secure channel
- Does not depend on a third-party tool or service
- Uses the native Windows Server service



Rather than using a Remote Desktop Connection to connect to a remote system directly, you can configure a Remote Desktop Gateway on the internal network. Then, you can configure the Remote Desktop Connection to connect to the Remote Desktop Gateway. This option can be configured in the Advanced tab of the Remote Desktop Connection tool.

If a remote connection is coming in from an external network, such as the Internet, you can use the Remote Desktop Gateway rather than individually configuring Internet connections through firewall on all remote desktop servers. It will handle the connection to the correct RDP server. This way, the remote desktop servers do not face the Internet but stay inside the internal network. The connection to the Remote Desktop Gateway is established using a secure channel.

One of the key benefits of Remote Desktop Gateway is that you don't have to add another third-party service. You can use this role on the Windows server as it uses the native RDP protocol on port 3389.



# *TOPIC 5*

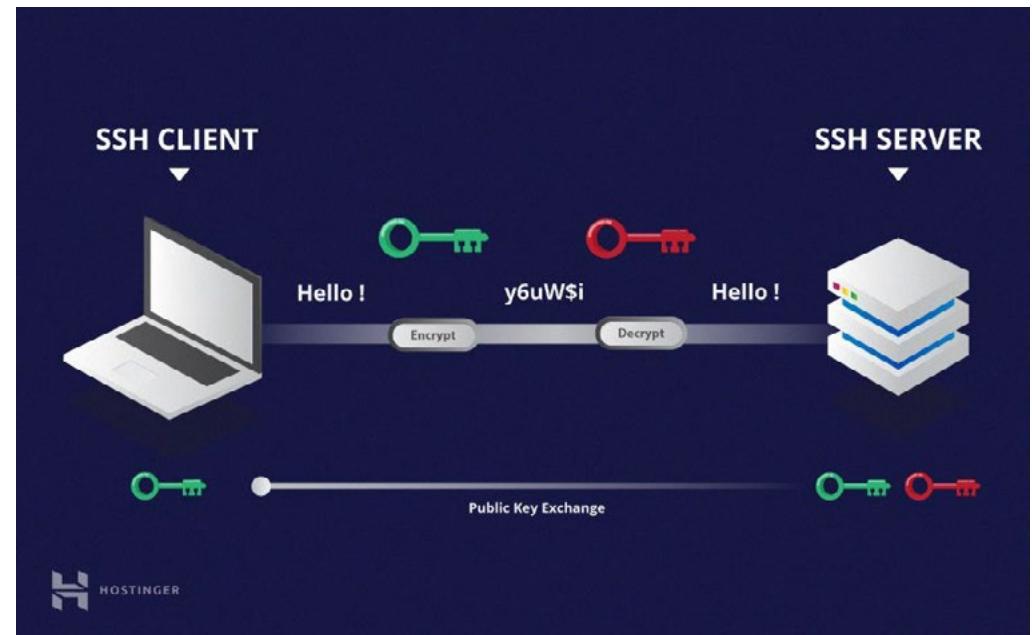
---

# SSH

---

# SSH

- Is used for remote terminal access
- Is a replacement to Telnet, which is a unsecure protocol
- Encrypts communication between endpoints
- Requires to be enabled on remote device or server
- Uses public key cryptography

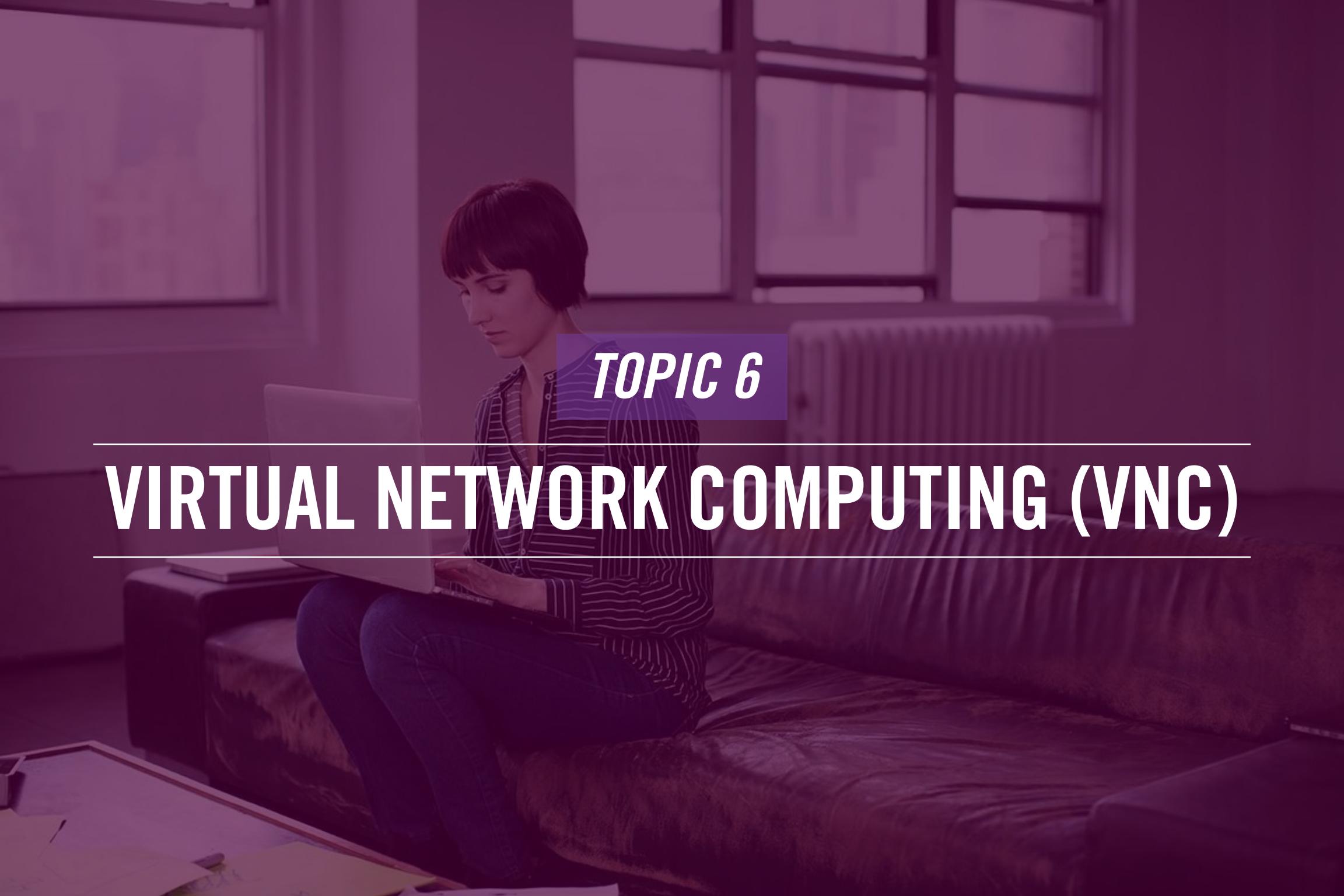


SSH or Secure Shell is a remote connection protocol primarily used on the Linux and Unix operating systems. In the good old days, Telnet was the protocol used for remotely connecting to Linux and Unix systems. However, the biggest security challenge with Telnet was that it transmitted the data, including the user credentials, in cleartext. SSH became the replacement for Telnet.

When you establish an SSH connection with a remote host, a secure channel is created. The secure channel ensures the integrity and confidentiality of the information being transmitted.

For SSH to work, you need to configure the destination system as the SSH server to accept the connections. The SSH client can then establish a connection with the remote server.

One of the good things about SSH is that it uses public-key cryptography that requires the SSH server or the destination system to have the public key. When a user attempts to connect with the destination system, the private key is then used. The combination of both the public and private keys are matched to authenticate the user. Remember that the private key never leaves the source system or the SSH client.

A woman with short dark hair is sitting on a brown couch, looking down at a laptop screen. She is wearing a striped shirt and jeans. The background shows a window with a grid pattern.

*TOPIC 6*

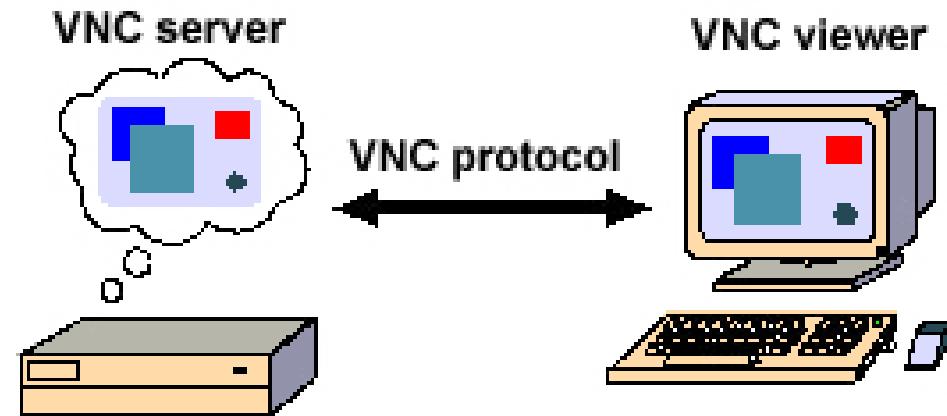
---

# VIRTUAL NETWORK COMPUTING (VNC)

---

# Virtual Network Computing (VNC)

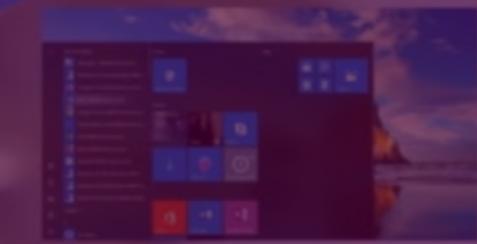
- Is used for remote desktop sharing
- Uses the Remote Frame Buffer (RFB) protocol
- Works with the client/server model
- Server – system that needs to be managed
- Client - system that will initiate the connection



Virtual Network Computing (VNC) works pretty much like Remote Desktop Connection. One of the good things about VNC is that it is platform-independent and can work with various operating systems. Several organizations and individuals use VNC to manage their systems remotely, and some even use it for troubleshooting the remote systems.

It provides remote desktop access to a user who initiates the connection. When a user connects to a remote system, the user gets to see the graphical interface of the remote system.

VNC makes use of the Remote Frame Buffer (RFB) protocol for creating a remote connection. RFB works similarly to the RDP protocol. You need to have a server on the destination system, and the source system uses the client, which initiates the connection to the server.



Microsoft Azure

# **TOPIC 7**

---

# VIRTUAL DESKTOP

---



# Virtual Desktop

- Run the user's desktop from a virtual environment
- Has less load on the user's system
- Helps to maintain a consistent environment from the virtual environment



Virtual desktops are operating system images that are remotely hosted and allow the users to interact with them as if they are using a desktop. Several devices, such as a mobile or a laptop, can be used as a client to access a virtual desktop. Typically, a client agent or software is installed on the mobile or laptop to connect to the virtual desktop.

With the use of virtual desktops, the client systems do not require a lot of computing power. They need a desktop, laptop, or mobile device to connect to the virtual desktop running on a remote system.

The virtual desktops can be configured to save changes or can discard changes when a user logs out. This way, the virtual desktop delivers a consistent environment every time a user logs on. For example, a user may log on from mobile and then from a desktop. The same virtual desktop is delivered to the user, which is a consistent experience.

*TOPIC 8*

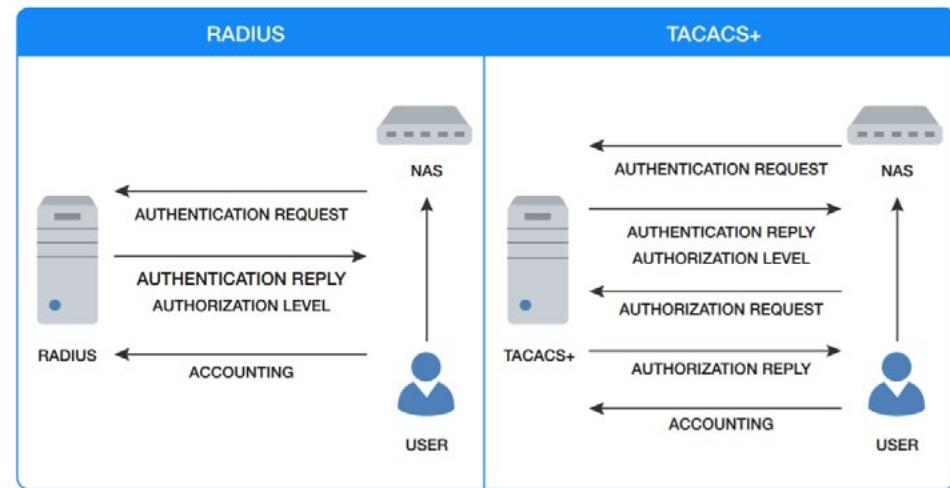
---

# AUTHENTICATION AND AUTHORIZATION CONSIDERATION

---

# Authentication and Authorization

- Use of AA
- RADIUS
- Use of AAA
- TACACS+
- Use of single sign-on (SSO)
- Use of Kerberos



There are several methods to authenticate and authorize a user over a network. The first method is Remote Authentication Dial-In User Service (RADIUS), which performs authentication and accounting. It combines authentication and authorization. In a nutshell, it performs two key functions – authentication and accounting and hence, is labelled as AA. Some people may label it under AAA for authentication, authorization, and accounting. RADIUS only encrypts the password and performs extensive accounting. It is used in cases where you need to authenticate users, such as client/server applications centrally. RADIUS uses the UDP protocol.

On the other hand, Terminal Access Controller Access Control System Plus (TACACS+) supports AAA, which is authentication, authorization, and accounting. It keeps accounting and authorization separate. Unlike RADIUS, which encrypts the password only, TACACS+ encrypts the entire data packet. It performs limited accounting. It works like RADIUS but keeps authorization separate. It is normally used with wireless access points and 802.1x compatible switches. TACACS+ uses TCP instead of UDP.

Single Sign-On (SSO) allows a user to authenticate once and access several applications in an enterprise environment. When a user logs on to the domain, the domain controller generates an access token and assigns to the user. The access token has a list of resources listed on which the user has access. When the user attempts to access a resource, the user's access token is verified for access. After a user logs on to the domain, several resources on which the user has access do not require the user to authenticate again.

Kerberos is another method of authenticating and authorizing users. When a user logs on to a system, the user's identity is established. Kerberos issues users tickets, and these tickets are like their gate passes to access resources. The tickets, however, are short-lived. They are refreshed as long as the user remains logged in.

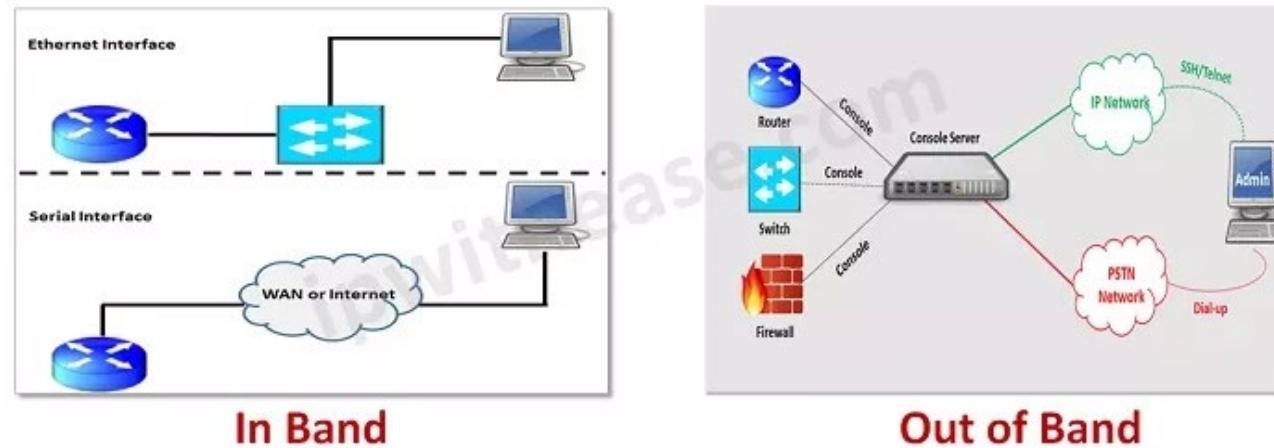
## *TOPIC 9*

---

# IN-BAND VS. OUT-OF-BAND MANAGEMENT

---

# In-band vs. Out-of-band Management



Most of the network administrators remotely connect to the servers using Telnet or SSH. This is known as in-band management. This method has been in use for a long time and is usually the preferred method of managing network servers and devices. In this method, the network traffic includes the management traffic. For security reasons, the management traffic should be segregated. For in-band management to work, the network must be up and running, and the server or device must be accessible.

Consider a server is down and has been switched off. You have no other option but to go and physical power it on. However, this problem is resolved with out-of-band management, which can handle a device when it is in:

- Powered down mode
- Sleep mode
- In hibernation
- Crashed

The out-of-band management provides an alternate method to work with the server without having to handle them physically. When a server is down, it is not possible to use the in-band management option. Then, you need to use out-of-band management, which ensures that you can still work with the devices when it is normally not accessible. Unlike in-band management, out-of-band management provides access via console, which use an IP address and port number.

The key feature of out-of-band management is that it works even when the network is down.

# Summary

- Site-to-site VPN
- Client-to-site VPN
- Remote desktop connection
- Remote desktop gateway
- SSH
- Virtual Network Computing (VNC)
- Virtual Desktop
- Authentication and Authorization Considerations
- In-band vs. Out-of-band Management

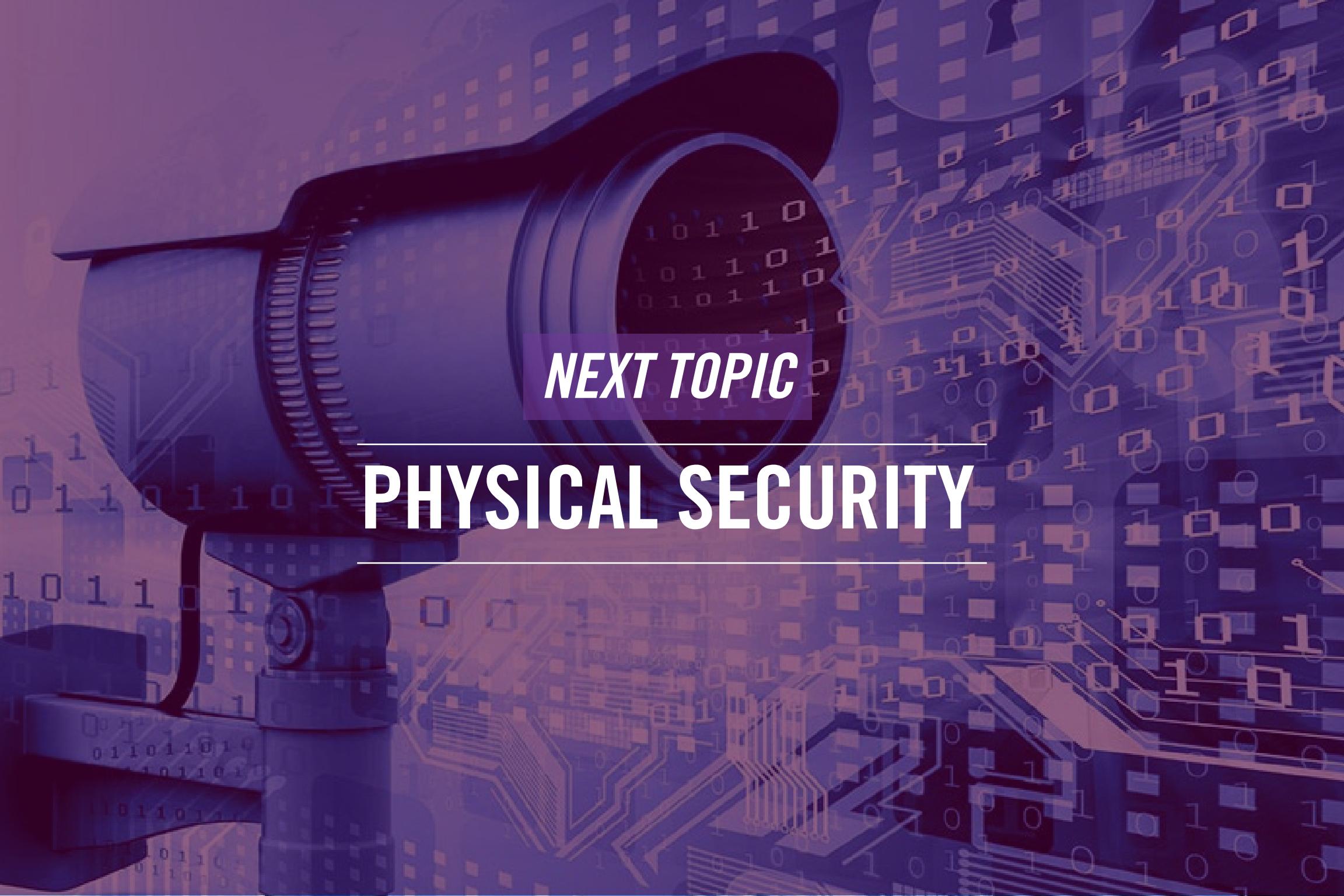


That's the end of the lesson.

Here we covered:

- |  |   |
|--|---|
| <ul style="list-style-type: none"><li>• Site-to-site VPN</li><li>• Client-to-site VPN</li><li>• Remote desktop connection</li><li>• Remote desktop gateway</li><li>• SSH</li></ul> | <ul style="list-style-type: none"><li>• Virtual Network Computing (VNC)</li><li>• Virtual Desktop</li><li>• Authentication and Authorization Considerations</li><li>• In-band vs Out-of-band Management</li></ul> |
|--|---|



A hand wearing a dark blue glove is holding a black computer mouse. The background is a dense, glowing blue and purple circuit board pattern with floating binary code (0s and 1s).

*NEXT TOPIC*

---

## PHYSICAL SECURITY

---

Lesson

# 5

# Physical Security

- 1 — Welcome to the 5 lesson of Module 4. In this lesson, you will learn about the:
- 2 — Physical Security



Network Fundamentals

# Agenda

- Detection Methods
- Prevention Methods
- Asset Disposal



Hi, welcome to COMPTIA Network+ Course  
In this lesson, we will talk about:

- Detection Methods
- Prevention Methods
- Asset Disposal



*TOPIC 1*

---

# DETECTION METHODS

---

# Cameras

- Serve as the detection method and serve as a deterrent control
- Are usually installed at the entry, exit, and critical area
- Can be of different types:
  - Fixed
  - Pan-Tilt-Zoom (PTZ)
  - CCTV



shutterstock.com · 1715110129

If you visit a shopping mall or any other building, you will notice CCTV cameras installed. These cameras are installed to detect any unwanted activity or person within that location. It is also possible to have guards placed, but then there is the cost factor. You will need multiple guards to monitor the big areas like a shopping mall. The guards may not monitor all corners of the mall or a large premise round the clock.

This is where cameras become extremely useful. You can install them, and then depending on the type of cameras they are. They can even record the movement of the people. In most cases, you will find the cameras installed at the entry and exit points. Organizations install the cameras in critical areas, such as the server room. Depending on the requirements of the organizations, different types of cameras can be installed. Some of the key types are:

- Fixed: Are installed on the walls in a fixed position to capture people's movement. They capture only the area because the camera cannot rotate.
- Pan-Tilt-Zoom: Are zoom cameras that can focus on an individual in a crowd.
- CCTV: Are cameras that can record videos, which can be saved for later viewing.
- IP-based: Are cameras that use the Ethernet cable to use Power-over-Ethernet (PoE). They can be managed using a mobile app or an application.

# Motion Detection

- Are used in high security areas within a facility
- Can perform various actions, such as:
- Send SMS
- Raise an alarm
- Light the area
- Can be of different types:
- Passive infrared (PIR)
- Electromechanical Systems
- Photoelectric Systems
- Acoustical Detection Systems
- Wave Motion Detector
- Capacitance Detector



Motion detection uses sensors to detect different types of motion. You typically install them in areas where you don't suspect any motion or maybe on odd hours, such as the middle of the night. You can install them in the server rooms, data centers, or emergency exits where you suspect the least activity at an odd hour. The way motion detection works is that it detects the motion of objects within a specific range.

It can then take different actions, depending on how it is programmed. When a motion of an object is detected, it can then perform one of the following actions:

- Send a message to the administrator or the designated authority
- Ring or raise the alarm
- Switch on the lights of the area

There can be different types of motion sensors. Let's quickly have a look at them.

- Passive infrared (PIR): Senses the changes in the heat waves.
- Electromechanical Systems: Detects the breakage in the electrical signal
- Photoelectric Systems: Detects the changes in lights
- Acoustical Detection Systems: Detects the unwanted sounds using microphones
- Wave Motion Detector: Generates a wave to check if anything disturbs it
- Capacitance Detector: Create a magnetic field to check if there is any disturbance to it

All these motion sensors can act to raise the alarm or perform any programmed action.

# Asset Tags

- Are bar-code stickers that are pasted on the assets
- Are RFID-based that can be used for electronic surveillance
- Can be scanned to get the details of the devices
- Can be:
  - Battery-powered
  - Passive



An asset tag is a bar-coded sticker pasted onto the assets, such as routers, switches, desktops, and laptops. Each asset tag has a number and several black-colored bars that uniquely identify the device. An asset tag is an RFID-based sticker that contains the complete information of the device is displayed from the database.

For example, when you scan the asset tag on a laptop, it contains information, such as:

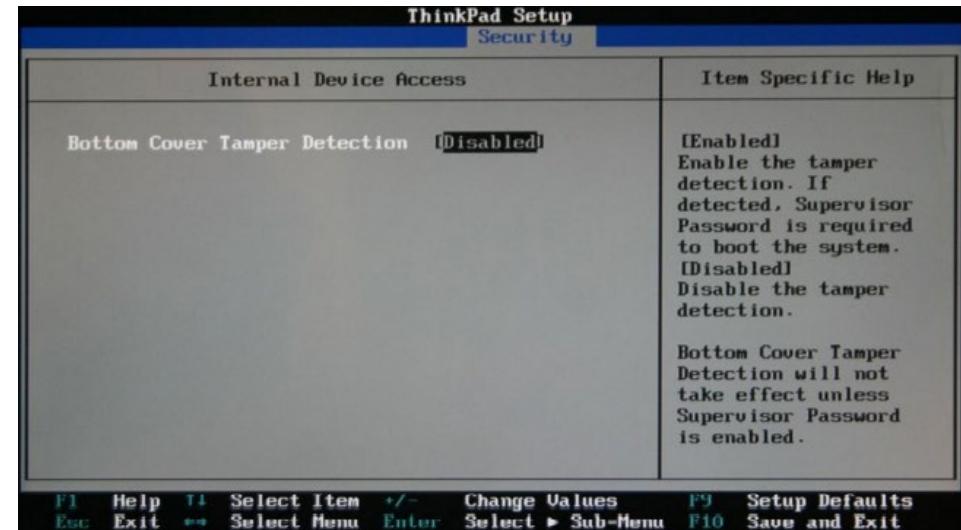
- Model number
- Make
- Purchase date
- Service information

An organization maintains a varied amount of information. Each RFID tag information is maintained in a central database. When the RFID tag is scanned, the information is displayed about the device or asset. The RFID tag can be pasted on the devices for asset inventory as well as electronic surveillance. When someone attempts to take these devices out, the sensors located at the entry or exit points of the office can detect these assets and update the database accordingly.

The asset tags can be either battery-powered or passive. The battery-powered, as the name suggests, use a battery to power themselves. On the other hand, the passive asset tags are stickers and do not have power. They need to be manually scanned.

# Tamper Detection

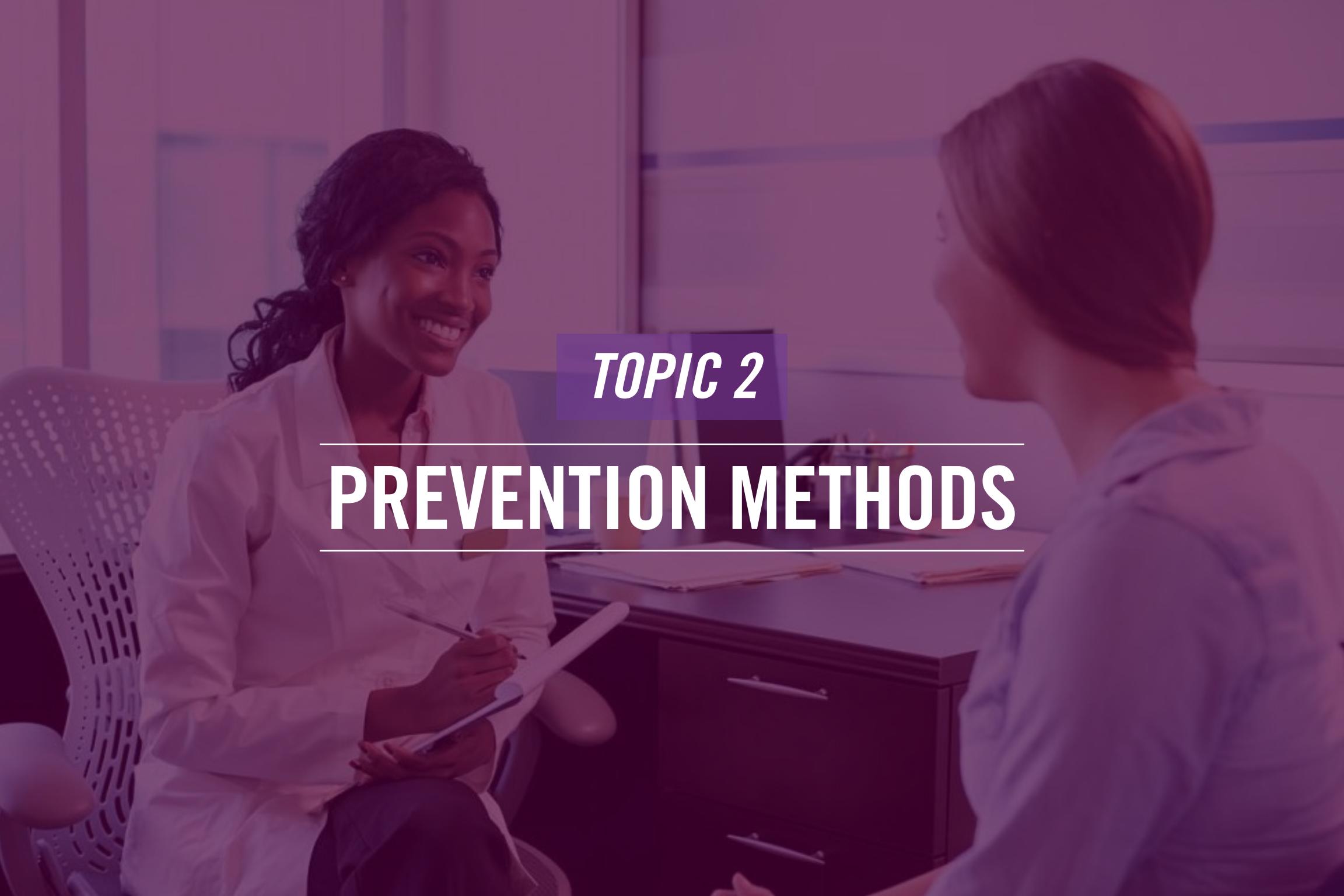
- Is a capability that a device has and can be configured in the BIOS settings
- Is used to protect intentional damage
- Can be found in:
  - Surveillance systems
  - Desktops and laptops
  - Printer cartridges
- Can alert a designated authority



Devices often have the tamper detection feature that the manufacturers enable. For example, several laptops and desktop BIOS has the tamper detection feature that is enabled by default. Manufacturers want to protect the devices from any intentional damage. If the user opens the laptop or desktop chassis, the user is notified of the unauthorized opening of the system, which leads to warranty voidness.

The tamper detection feature is enabled on various devices, such as surveillance systems, desktops, laptops, and printer cartridges. For example, if you have used HP cartridges, they have the tamper detection feature. If you open the cartridge to refill it yourself and close it, the printer can detect using counterfeited cartridges.

Other than the user, this feature can also alert the designated individuals or the manufacturers.

A photograph of two women in a classroom or office setting. One woman, on the left, is smiling and writing in a notebook. The other woman, on the right, is facing away from the camera. The background shows desks and papers.

*TOPIC 2*

---

## PREVENTION METHODS

---

# Employee Training

- Is conducted to make users security aware
- Can also be conducted to educate users about various subjects
- Can be done in various ways:
  - Demonstrations
  - Lunch and learn
  - Training Videos
  - Awareness Events
  - Trainings



Users are one of the most important assets of an organization. Nowadays, they are the key target for attackers. They need to be trained properly to ensure that they do not remain the weakest link in the security chain. Think of a scenario where an organization puts in all the possible security devices and applications and secures the network. However, one user falls victim to a phishing email, and that would be all. There is a high possibility that the attacker would have the capability to take down the network. The core intent of the employee training is to make their security-aware. Remember, you are not focusing on making them security experts, but they need to know the fundamentals to understand the dos and don'ts. You should educate them on various subjects like phishing, social engineering, SPAM, and so on to ensure that these attacks are targeted towards them, and therefore, they should know about these fundamental concepts.

Different organizations may use different methods to train their employees. Let's look at some of the possible methods.

- Demonstrations: Employees are shown various concepts in the form of demonstrations. A good example to demonstrate to the employees is password cracking to highlight how simple passwords can be cracked in seconds.
- Lunch and Learn: You can organize a training session during the lunch break where the employees have lunch and learn the concepts.
- Training Videos: You have to record training videos and host them inside your organization. It is more like a YouTube concept where the employees can go and watch the videos. The videos are typically hosted on a Learning Management System (LMS) that can help you track the employees' progress on the videos.
- Awareness Events: Rather than making generic security sessions, you can have awareness events focused on specific topics. For example, you can host an awareness event on phishing or social engineering.

Training: Training is typically longer in duration that can last from one day to a few days. Various concepts are covered.

# Access Control Hardware – Badge Readers

- Are RFID-based that are flashed in front of a proximity reader to detect credentials
- Are used for authentication purposes
- Transmit the badge number to the proximity reader to authenticate the user
- Are used for entering a restricted location, such as a data center or server room



Have you ever flashed your organization's ID card in front of a device to open a door or maybe mark attendance? The device to which you are flashing your ID card is a badge reader, an RFID-based device. Within specific proximity, it can detect the ID card or the badge and read its information.

Each RFID card has a unique identification code that identifies it. When the card is flashed in front of the badge reader, it reads through the information inside the card and then checks the database for permissions. Such permissions are marked in the database for the RFID reader. Based on the permissions, it then allows or denies access to a specific entrance. For example, a user has access to the main office entrance but does not have permission to open the data center door. In short, it is authenticating the user – similar to what Windows does when providing a correct or incorrect password.

You do not install badge readers all over the office building. You would install them at a specific location where you want to restrict the user entry.

# Access Control Hardware – Biometric Locks

- Use the physical characteristics of the user to authenticate
- Are used for authenticating users to enter a facility or room
- Can be used in multi-factor authentication:
  - Something you know: Password or Pin
  - Something you are: Physical characteristics, such as retina or fingerprint



Have you ever performed a fingerprint scan to open a door? If yes, you have used the biometric lock. The biometric devices are used for authenticating the users based on their physical traits, such as retina or fingerprint. For example, it can be a biometric lock requiring a fingerprint scan to unlock the door. It can also be a biometric lock to perform a retina scan or perform facial recognition.

Each biometric lock is linked to a central database that maintains the user credentials, consisting of the retina scan, fingerprints, or even the facial scans. Using whichever biometric method a user attempts to authenticate, the centralized database is checked and based on the match. The user is either allowed or denied access.

It is also quite common to have the biometric method be clubbed with another method, such as password or PIN. When both the methods are used together, it is the two-factor authentication. You can combine methods, such as something you know – a password or a PIN and something you are – your physical traits, such as a fingerprint.

# Locking Racks

- Is a method of protecting the physical assets residing in the racks
- Can be locked with biometric, manual, or RFID-based locks
- Are opened with swinging a handle that can be used after unlocking



The administrators often pay attention to the data center is locked but not the racks inside it. To secure the assets inside the racks, you need to ensure that they are locked. Think of the worst that can happen – if someone piggybacks you inside the data center or someone breaks into it, there should be another level of protection for the assets inside the racks. If racks are left open, it is easy for the attacker to pick up a few assets and walk away. However, if there are locks of whichever kind, they can serve as the second level of protection.

Usually, racks have different types of locks, which can be biometric, manual, or RFID-based. Depending on your need, you should get any of these locks.

Depending on the type of lock on the rack, you need first to unlock it. It could be a manual lock that you need to open with a key, or it could be a biometric lock. After you unlock it, you need to pull the swinging handle and rotate it to open the rack door.

# Locking Cabinets

- Is required to safeguard the physical material, such as:
  - Documents
  - Laptops
  - Hardware
- Can be done using manual or digital locks



Other than the racks in the data center, an organization can have several cabinets to store other types of assets, such as documents, laptops, or hardware, which can be routers, wireless access points, or keyboards. Most of these assets, such as documents, can be critical and confidential to your organization. Therefore, you need to protect them. You need to properly store them in the cabinets, which should be protected with a lock, manual or digital.

# Access Control Vestibule

- Is also known as mantrap
- Is installed to prevent tailgating and piggybacking
- Allows only one person to enter and exit at any given point of time
  - Person needs to authenticate before exiting
  - Second person is allowed after first person exit



Tailgating and piggybacking has always been a problem for organizations. In tailgating or piggybacking, one user authenticates to enter a room, and then the second one follows without authentication. This is because the door is open, and it is easy for the second user to sneak in following the first one. This leads to a problem of unauthorized users entering an area where they should not be present.

Several organizations often use Access Control Vestibule, which is also known as mantrap. The main purpose of using a mantrap is to prevent tailgating or piggybacking. There are two doors, an entry and an exit. When a user enters the mantrap, the entry door behind the user closes. After the user exits the mantrap, another user is allowed to enter. To exit the mantrap, the user has to authenticate himself to unlock the exit door.

# Smart Lockers

- Are digitally capable lockers that can work with:
  - NFC
  - RFID
  - Touch pads
- Are used for delivery purposes
  - Recipient can be notified when the package arrives
  - Recipient receives the access instructions



Smart lockers are now becoming popular with users. Suppose you need to deliver a package to the person this afternoon, but the person is not available till tomorrow morning. You can use the smart locker to deliver this package. Smart lockers are usual lockers that individuals can rent for various purposes like the delivery of an item. However, these are called smart lockers as they have several features that normal lockers do not. They work with an intelligent process of sending instructions and notifications to the recipients.

Let's continue with the package delivery that you are supposed to make. You leave the package in a smart locker, which notifies the recipient that the package has arrived. In the notification, there are access code and smart locker operating instructions. The recipient can use this information to collect the package. You also get notified when the package is collected. The smart lockers are protected with NFC-based locks, RFID-based locks, or touchpads.

The background image shows a stack of old computer equipment against a cloudy sky. It includes a CRT monitor, a keyboard with a checkered pattern, and a tower unit with various cables and drives.

*TOPIC 3*

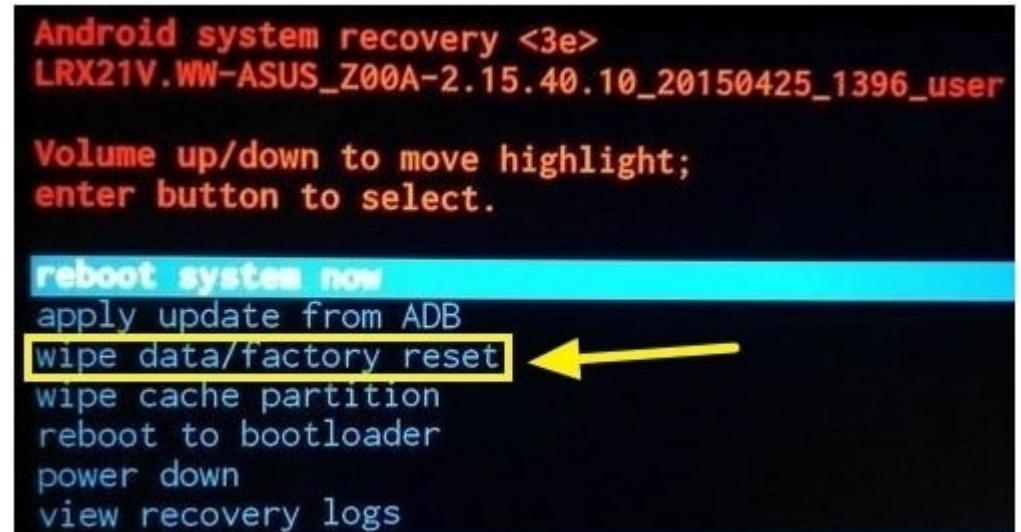
---

# ASSET DISPOSAL

---

# Factory Reset/Wipe Configuration

- Resets the device to original configuration when it was delivered from the factory
- Brings back original factory delivered applications and configuration settings but removes user's configuration and data
- Is generally used:
  - When you want to get the original settings back due to a technical issue
  - Want to discard the device without the configuration settings



When you purchase a device, such as a router or a laptop, it comes with certain configuration settings defined by the manufacturer. You can custom configure the devices based on your requirements. However, when you are disposing of the devices, you need to ensure that the custom configuration should be erased. To do this, you can reset the device to the original configuration present on the device when it was delivered from the factory.

When you do the factory reset, the custom configuration is wiped off. The factory configuration is brought back on the device. This should be standard practice before asset disposal. One of the key reasons is that you do not want the configuration to fall into the wrong hands. For example, you dispose of a laptop without performing a factory reset. An attacker gets his hands onto the laptop, and then he can recover a lot of information that can serve him a fortune.

- You would typically perform a factory reset because:
- There is a technical issue, and you want to revert to the factory settings and start over
- You need to dispose of the device without the custom configuration

# Sanitize Devices for Disposal

- Is used when disposing a device, such as:
  - Hard drive
  - Optical media
  - CD/DVD
- Can be done using various methods, such as:
  - Data overwrite
  - Data wipe
  - Degaussing
  - Encryption scramble
  - Physical destruction



Storage devices can turn into culprits after you insecurely dispose of them off. In most cases, the users delete the data from a hard drive or USB before handing it off to another person. However, this information can always be retrieved. To ensure data privacy, the data must be securely wiped off from the storage devices. Cases like CDs or DVDs can be scratched and broken into pieces to prevent data from being recovered.

Several methods can be used for removing data from storage devices like hard drives. Some of the key methods are:

- Data overwrite: Overwrite the existing data with new data. As new data keeps overwriting the old data, the chances of data recovery reduce.
- Data wipe: Overwrite the data with binary values 0 and 1. Once a data wipe is performed, previous data cannot be recovered.
- Degaussing: Destroys the data using a magnetic force.
- Encryption Scramble: Scrambles the data in an unreadable format and removes the encryption key.
- Destruction: Destroys the hard drive physically.

# Summary

- Detection Methods
- Prevention Methods
- Asset Disposal



That's the end of the lesson.  
Here, we covered:

- Detection Methods
- Prevention Methods
- Asset Disposal



The background of the slide features a stylized globe of the Earth, rendered in shades of blue and purple. Overlaid on the globe are numerous glowing, translucent lines of varying colors (blue, orange, red) that represent network connections or data flow. These lines form a complex web that covers the entire globe, symbolizing global connectivity and technology.

*NEXT TOPIC*

---

## NETWORK TROUBLESHOOTING METHODOLOGY

---

---

# MODULE 5

---

# Module 5

- LESSON 1 [NETWORK TROUBLESHOOTING METHODOLOG](#)
- LESSON 2 [TROUBLESHOOT CABLE CONNECTIVITY ISSUES](#)
- LESSON 3 [NETWORK TOOLS AND COMMANDS](#)
- LESSON 4 [WIRELESS CONNECTIVITY ISSUES](#)
- LESSON 5 [TROUBLESHOOTING NETWORKING ISSUES](#)



Lesson

1

---

# Network Troubleshooting Methodology

- 1 — Welcome to the first lesson of Module 5. In this lesson, you will learn about the:
  - 2 — Network Troubleshooting Methodology
- 



Network Fundamentals

# Agenda

- Identify the problem
- Establish a theory of probable cause
- Test the theory to determine the cause
- Establish a plan of action to resolve the problem and identify potential effects
- Implement the solution or escalate as necessary
- Verify full system functionality and, if applicable, implement preventive measures
- Document findings, actions, outcomes, and lessons learned



Hi, welcome to COMPTIA Network+ Course

In this lesson, we will talk about:

- Identify the problem
- Establish a theory of probable cause
- Test the theory to determine the cause
- Establish a plan of action to resolve the problem and identify potential effects
- Implement the solution or escalate as necessary
- Verify full system functionality and, if applicable, implement preventive measures
- Document findings, actions, outcomes, and lessons learned



A photograph of a group of people working together in an office or study environment. In the foreground, a man with short brown hair, wearing a denim jacket over a striped shirt, is focused on a laptop screen. Behind him, several other individuals are seated at desks, also working on their computers. The background shows shelves filled with books and papers, creating a professional and collaborative atmosphere.

*TOPIC 1*

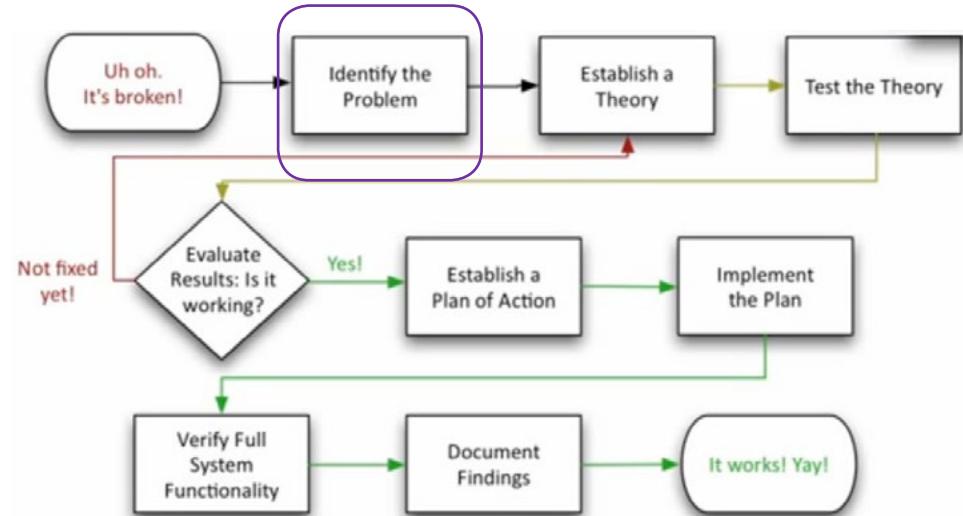
---

# IDENTIFY THE PROBLEM

---

# Identify the Problem

- Gather information
- Question users
- Identify symptoms
- Determine if anything has changed
- Duplicate the problem, if possible
- Approach multiple problems individually



As and when a problem occurs, you should not rush into implementing a solution. You need first to identify the problem. This is the first step in troubleshooting a problem. There are proper steps that need to be followed to conclude that the problem has been solved. However, as the first step, you need to know what the problem is. Without knowing the problem, you may implement a wrong solution, which may further complicate the problem.

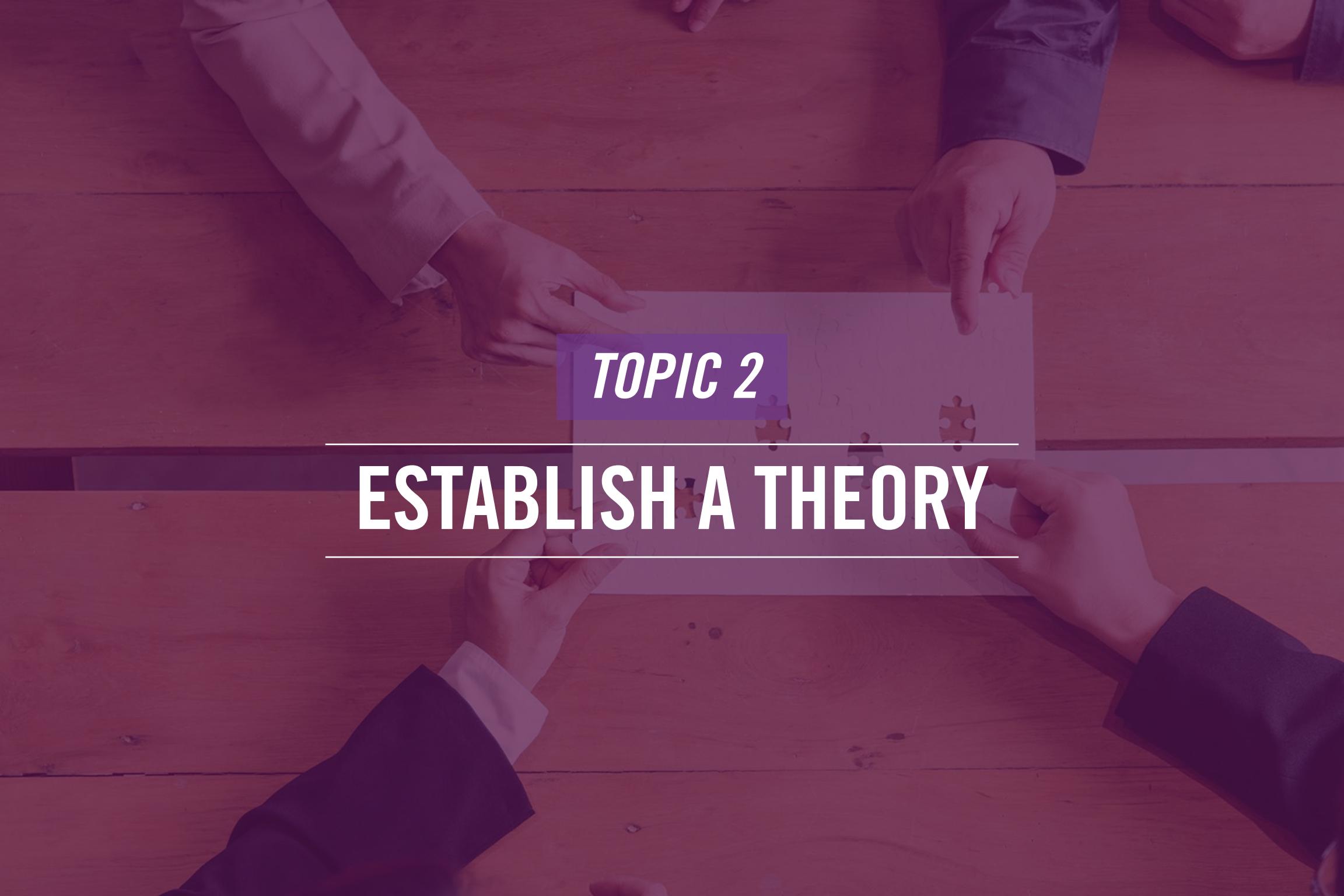
Various tasks need to be performed in this step. You need to gather as much information as possible about the problem that has occurred. You should also question the users. They can provide some valuable inputs. For example, what action did the user perform after which the problem occurred? A user might tell that the system has been unstable since the display drivers update. This is a good insight to know. It might not be the real problem, but it surely throws a hint that the problem could be due to the display drivers.

You need to identify the symptoms then. For example, if the system cannot connect to the network resources, you can investigate if the system is getting an IP address in the first place.

Going back to the display drivers' example, you can determine if anything has changed in the system due to the problem.

You can also try to duplicate the problem. However, this may not be possible in all scenarios, but it might give good insights into why the problem occurs.

As the last task in this step, you need to isolate the problems. You may have to break a bigger problem into several smaller ones. It is necessary to tackle each problem individually, not as a collective one.

A photograph showing several pairs of hands reaching across a light-colored wooden table to assemble a large, rectangular puzzle. The puzzle pieces are white with black outlines. In the center of the puzzle, the words "TOPIC 2" are printed in a bold, white, sans-serif font.

**TOPIC 2**

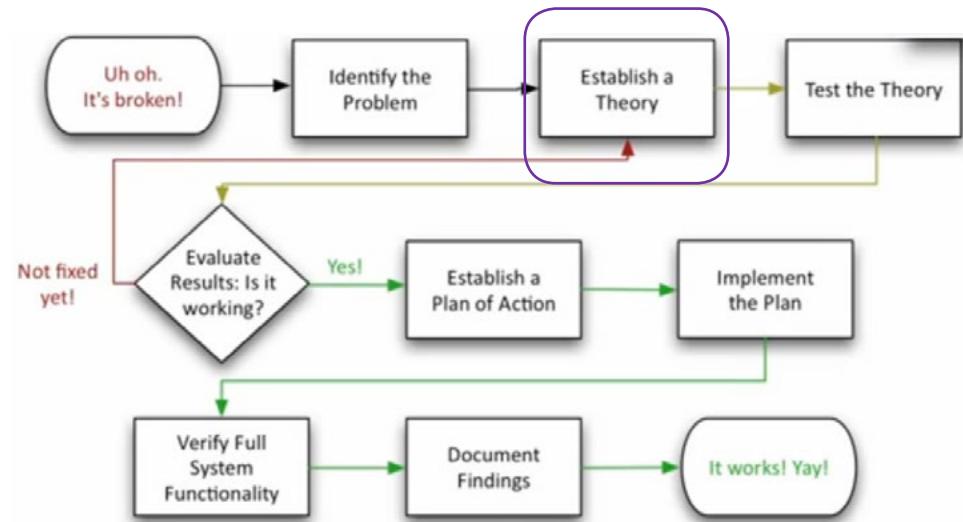
---

# ESTABLISH A THEORY

---

# Establish a Theory

- Question the obvious
- Consider multiple approaches
  - Top-to-bottom/ bottom-to-top OSI model
  - Divide and conquer



After you have identified the problem, you need to establish a theory now. Two key tasks need to be performed in this step. You need to start with the obvious. For example, if a system is not booting up – does the system have power? If yes, is it getting powered on? If something is looking obvious, do not avoid it. It could be a problem with the power cord that is faulty and due to which the system is not able to power on. The system not getting powered on seems like a huge problem, but the solution is rather smaller. So, do not ignore the obvious and check it out if it could be an answer to the problem.

You can also refer to the top-to-bottom or a bottom-to-top model approach related to the OSI model. The problem has to be at one of the OSI layers. You can try to find out on which layer does the problem exists. For example, the name resolution problem is related to DNS, which functions at Layer 7. You now know that the problem is not in the remaining six layers but Layer 7.

When a problem occurs, you can also use the divide and conquer approach. You can ask the team to split and find the solution. Each individual can be assigned a specific task. The outcome is that now you have several individuals trying to find the solution – more brains – more solutions. The chances are that you are likely to find the problem much more quickly.

## *TOPIC 3*

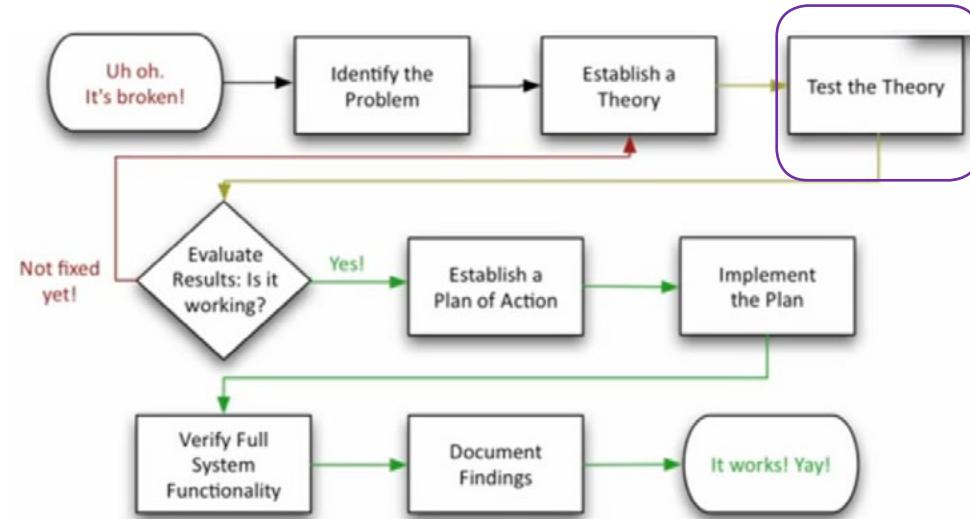
---

# TEST THE THEORY

---

# Test the Theory

- If the theory is confirmed, determine the next steps to resolve the problem
- If the theory is not confirmed, reestablish a new theory or escalate



After you have established the theory, it is time to move ahead and test the theory. This is the next step. The theory may or may not work. Some theories will work as you had thought them. They would do. However, some theories will fail.

Whether the theory works or not, it can be validated only when you test the theory. If the theory works as it was thought to work, you can proceed to the next step in solving the problem. For example, if you have tested the found that the system is not powered on, you developed a theory that the power cable is bad. You test the power cable with another system. You are validating the theory. If the cable does not power on the second system, your theory is proven to be correct. If it powers on, then you know that your theory is not correct. You will have to go back and re-establish another theory.

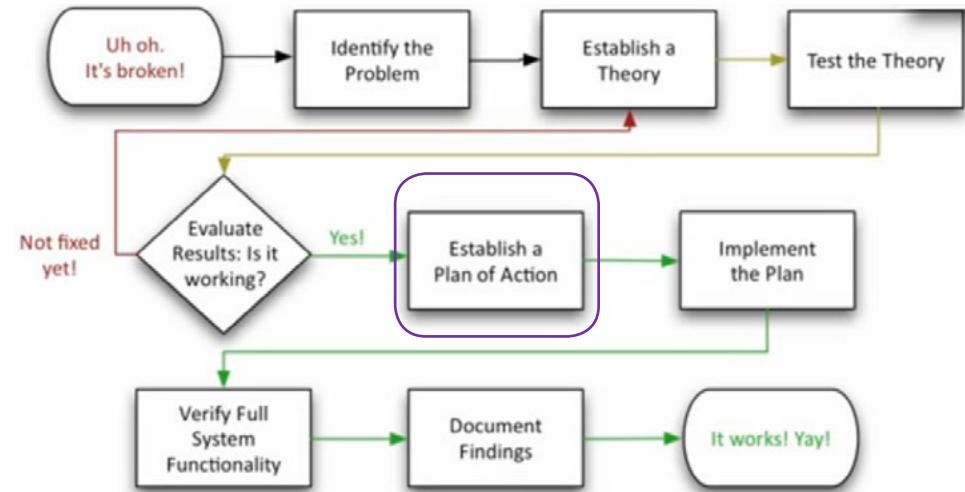
## TOPIC 4

# ESTABLISH A PLAN

M	T	W	T	F	S	S
2	3	4	5	6		
9	10	11	12	13		
16	17	18	19	20		
23	24	25	26	27		

# Establish a Plan

- Determine the possible effects of the solution that you plan to implement
- Need to determine a workaround or a final solution

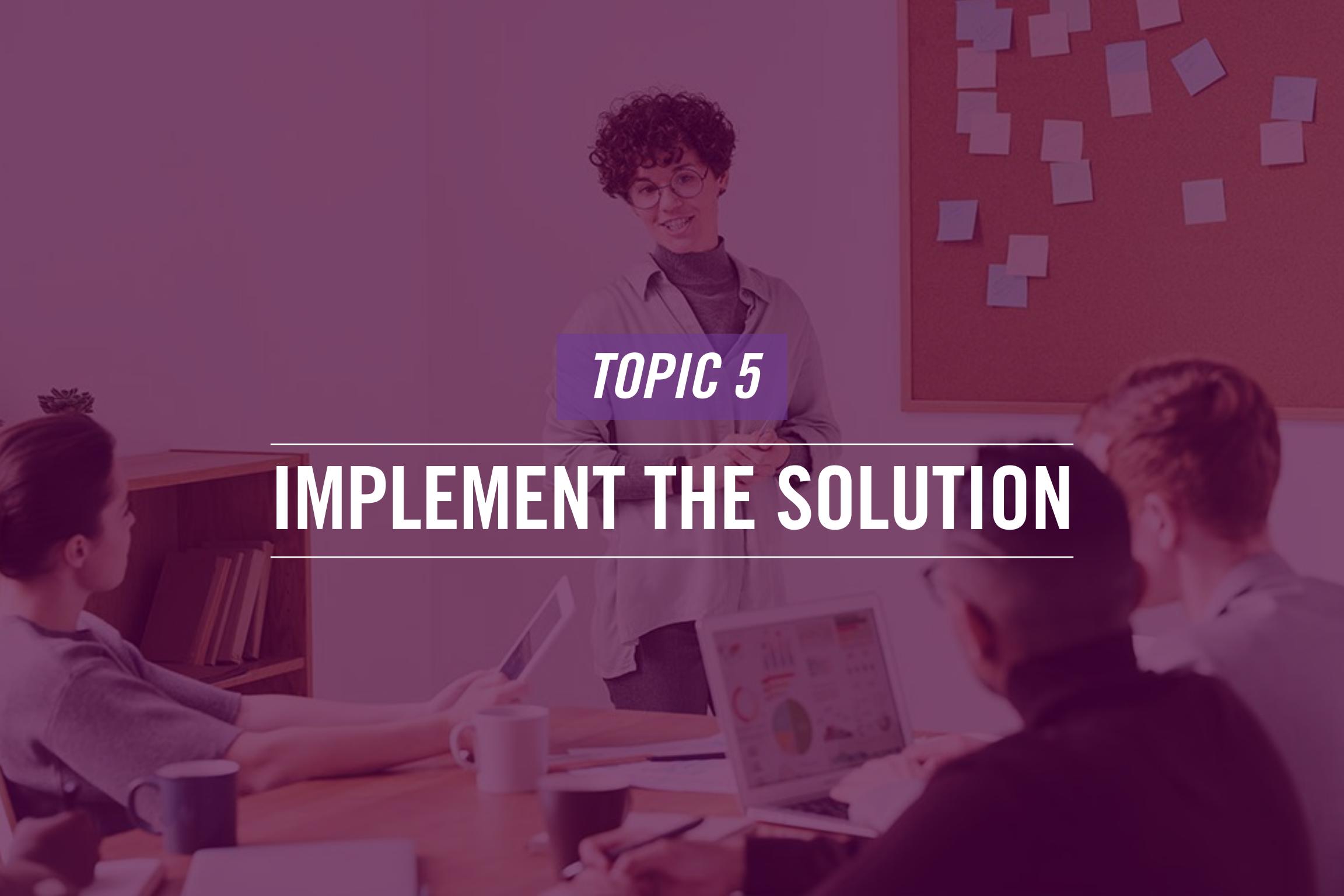


[Troubleshooting Introduction - Mahara](#)  
[muirfield-h.schools.nsw.edu.au](http://muirfield-h.schools.nsw.edu.au)

The next step is to establish a plan. If your theory proves to be correct, it is time to move ahead and establish a plan. It is important to plan the solution for the problem being faced. For example, you need to plan and determine the overall impact of the scenario carefully. Depending on the nature of the problem, the solution may be a simple or a complex one. It may take a short or long time to implement – if this happens, can the problem be handled with a workaround.

To tackle the problem or the issue, you need to create a step-by-step plan, including the possible negative impacts of the solution you will implement. You also have to determine if the solution closes the problem but creates another one. For example, a patch may close one vulnerability but may cause application stability issues.

If this scenario occurs, you need to discard the solution and find an alternative to fix the solution.

A photograph of a professional meeting. A woman with curly hair and glasses, wearing a grey blazer over a turtleneck, stands in the center, smiling and gesturing with her hands. She is surrounded by four other people: a woman on the left looking at a tablet, a man in the foreground writing on a notepad, a woman on the right looking at a laptop, and a man in the background looking towards the camera. They are seated around a light-colored wooden conference table. In the background, there's a whiteboard with several blue sticky notes pinned to it.

## *TOPIC 5*

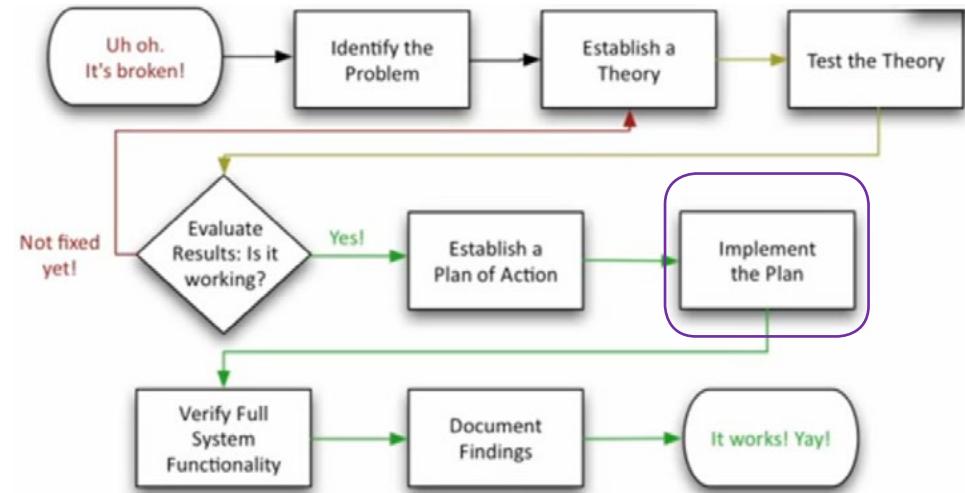
---

# IMPLEMENT THE SOLUTION

---

# Implement the Solution

- Implement the plan that you created in the previous step
- Need to have requisite permissions to implement the solution
  - May require additional help



[Troubleshooting Introduction - Mahara](#)  
([muirfield-h.schools.nsw.edu.au](http://muirfield-h.schools.nsw.edu.au))

So, you have completed the planning step in the troubleshooting methodology, and it is time to move ahead to implement the solution. The solution needs to be based on the plan that you had created earlier. You cannot do it alone. There will be scenarios where even though you have to implement the solution. For example, you may depend on another team to replace a router as it is not your core expertise. It can also be another scenario where you have to add a route to resolve a routing problem for a specific subnet.

You may also require additional permissions or privileges to implement the solution. For example, you need to reset the password for a specific user or implement the account lockout policy. The Active Directory Administrator's help is required to do these tasks, which is fair enough. In large organizations, the responsibilities are divided, and therefore, a lot of team coordination is required.

You may also have to get additional help. You can partially implement the solution, but then a senior engineer with more knowledge is required to validate the implemented solution.

A photograph of a woman with long dark hair, wearing a white t-shirt, sitting at a desk and working on a silver laptop. She is looking down at the screen. On the desk next to her is a white mug. The background is slightly blurred.

## *TOPIC 6*

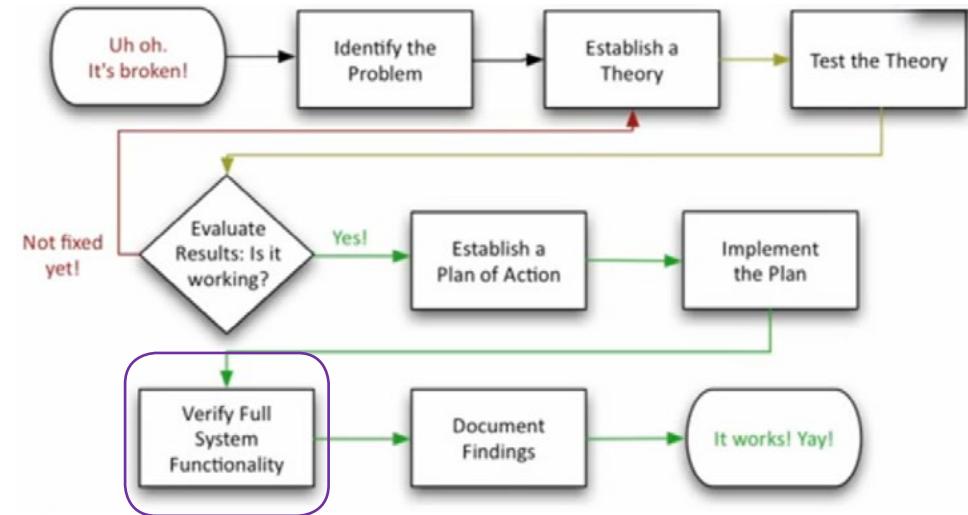
---

# VERIFY THE FUNCTIONALITY

---

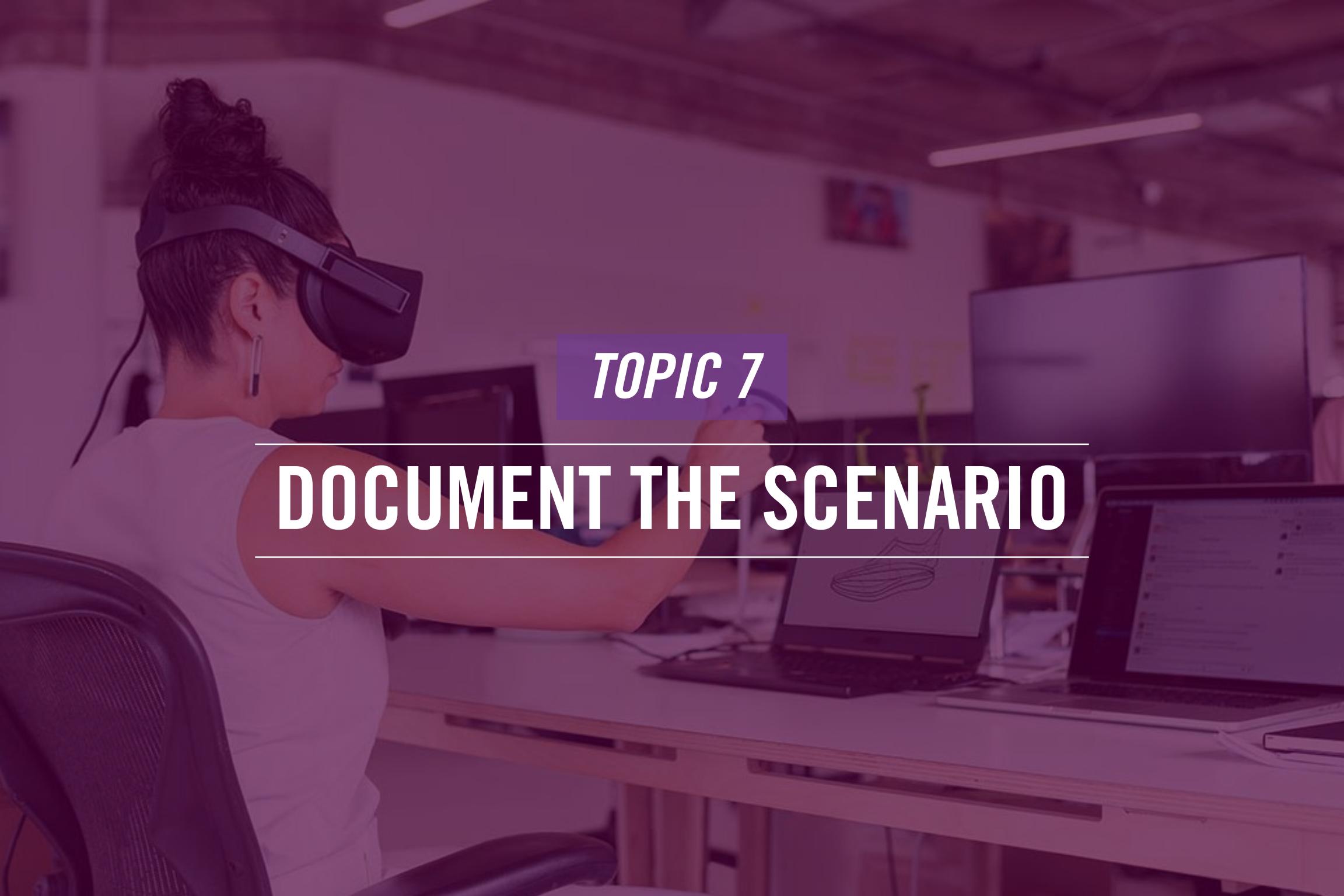
# Verify the Functionality

- Is the next step after implementing the solution
- Requires the validation of the solution implemented
  - Ensure there are no negative outcomes
  - Ensure the problem is fixed
- Implement preventive measures



After you implement the solution, you need to verify the functionality. This is required because the current problem may be fixed, but another problem may crop up as an outcome. Therefore, the implemented solution needs to be verified.

You have to ensure that there are no negative outcomes and the current problem is fixed. You may have to implement preventive measures to ensure that the problem does not occur again. For example, users may be receiving a lot of SPAM. It is a recurring problem that you want to prevent. So, as a preventive measure, you implement a SPAM filter to reduce the amount of SPAM that the users get.

A person with dark hair tied up in a bun is wearing a VR headset and holding a VR controller. They are seated at a desk with multiple computer monitors. One monitor shows a 3D model of a shoe. The background is a blurred office or lab environment.

## *TOPIC 7*

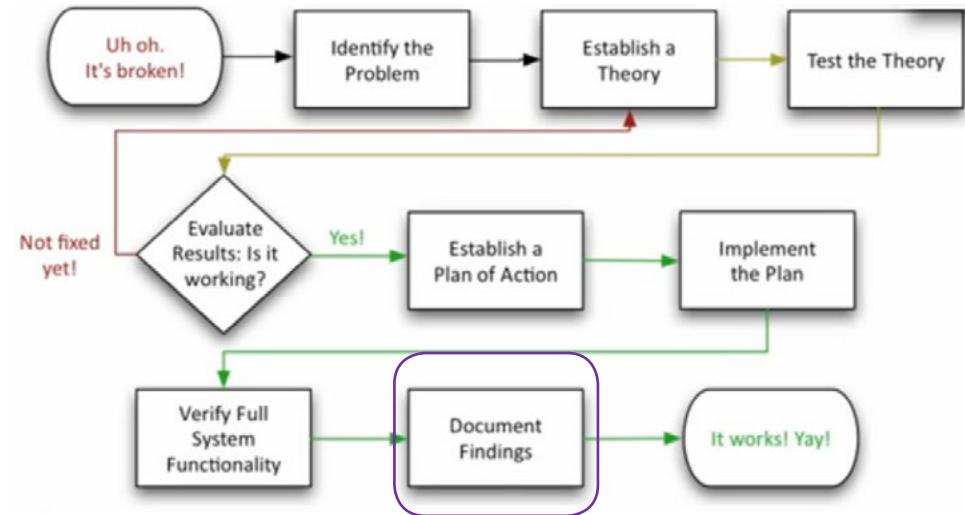
---

# DOCUMENT THE SCENARIO

---

# Document the Scenario

- Requires the document to be created/updated based on a new or existing problem
- Requires new document if:
  - Problem is new
  - Problem has never encountered before
- Should capture the following:
  - Symptoms
  - Corrective actions
  - Outcomes



In the troubleshooting methodology, documentation is the final step. You encountered a problem, verified it, and then came up with a theory to implement a solution. After the implementation, you need to document the problem and solution now. There may be existing or outdated documentation on the same problem, but you need to update the document.

If the problem is occurring for the first time, you need to document it with the solution. If the problem is a recurring one, you may have to update the documentation. For example, the network connectivity issues were a problem with a specific type of network adapters. However, with a patch, the issue was resolved. The same problem occurred with another type of network adapter. You may have to look for a patch for this network adapter. Rather than creating a new document, you can amend the existing document and update it with the new network adapter and its patch details.

When you are documenting the problem, be sure to implement the following:

- Symptoms
- Corrective actions
- Outcomes

# Summary

- Identify the problem
- Establish a theory of probable cause
- Test the theory to determine the cause
- Establish a plan of action to resolve the problem and identify potential effects
- Implement the solution or escalate as necessary
- Verify full system functionality and, if applicable, implement preventive measures
- Document findings, actions, outcomes, and lessons learned



That's the end of the lesson.

Here we covered:

- |   |  |
|---|--|
| <ul style="list-style-type: none"><li>• Identify the problem</li><li>• Establish a theory of probable cause</li><li>• Test the theory to determine the cause</li><li>• Establish a plan of action to resolve the problem and identify potential effects</li></ul> | <ul style="list-style-type: none"><li>• Implement the solution or escalate as necessary</li><li>• Verify full system functionality and, if applicable, implement preventive measures</li><li>• Document findings, actions, outcomes, and lessons learned</li></ul> |
|---|--|

The background features a stylized globe of the Earth with a network of glowing blue and orange lines representing connectivity or data flow. The globe is set against a dark, textured background that looks like a starry sky or a digital grid.

*NEXT TOPIC*

---

## TROUBLESHOOT CABLE CONNECTIVITY ISSUES

---

# 2

---

# Troubleshoot Cable Connectivity Issues

- 1 — Welcome to the 2 lesson of Module 5. In this lesson, you will learn about the:
  - 2 — Troubleshoot Cable Connectivity Issues
-

# Agenda

- Specifications and limitations
- Cable considerations
- Cable application
- Common issues
- Common tools



Hi, welcome to COMPTIA Network+ Course

In this lesson, we will talk about:

- Specifications and limitations
- Cable considerations
- Cable application
- Common issues
- Common tools



A photograph showing several people from behind, focused on a task. One person in the center-left is holding a white tablet with a grid of colored icons on its screen. Another person's hands are visible at the bottom left, writing on a large sheet of paper with a pen. A third person's hands are at the bottom right, also writing on the same or a nearby sheet. They appear to be in a workshop or classroom setting, with various papers and a calculator visible.

## *TOPIC 1*

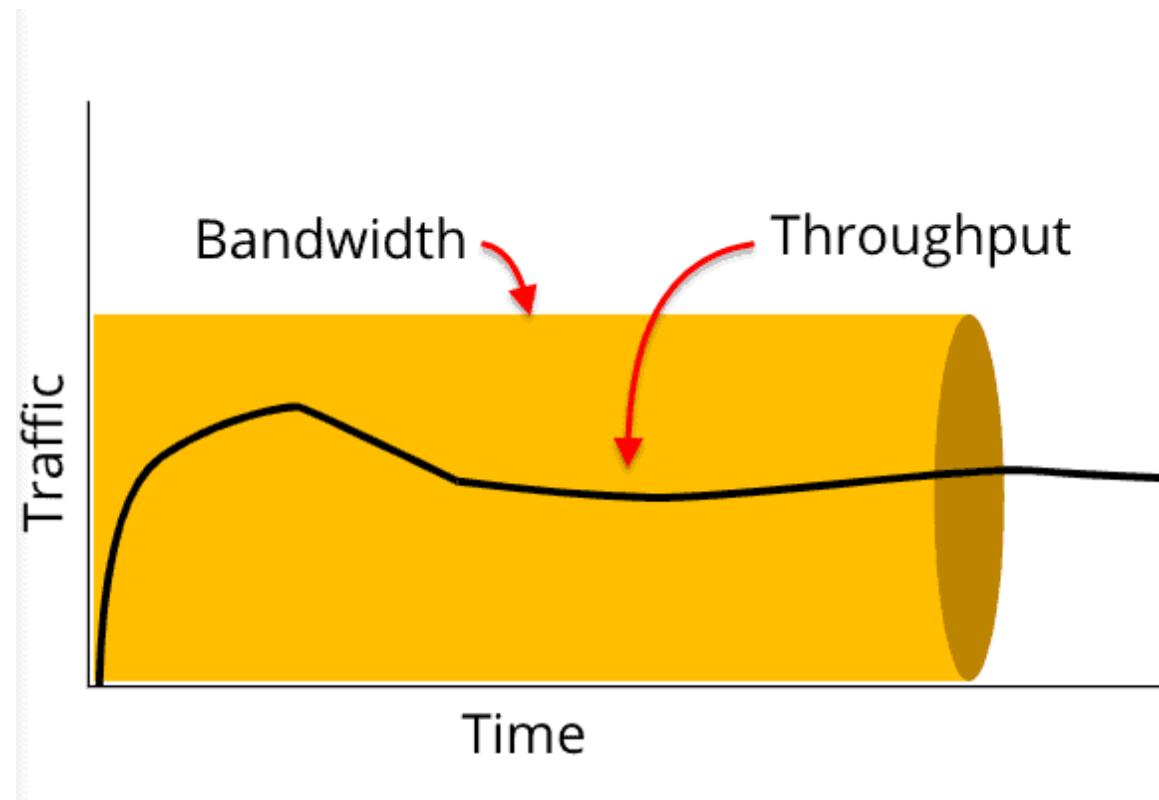
---

# SPECIFICATIONS & LIMITATIONS

---

# Throughput

- Is impacted due to several reasons
  - Jitter
  - Latency
  - Packet loss
- Can be tested using throughput tester



Throughput is the amount of data sent from one system or device to another in a specific time frame. Throughput is one of the most common issues in a network. It can occur due to jitter, latency, and packet loss on a network. If you suspect that there is slow throughput, you need to monitor the network interface and verify the throughput, which can be done with a throughput tester available on the Internet. They measure the throughput from the source to the destination.

When you face slow throughput, you may have to pay attention to reducing the latency, jitter, or packet loss, which eventually will increase the throughput. When referring to throughput, it is often confused with bandwidth. Throughput is the amount of data that flows out. You measure the throughput, which means working in a real-life scenario. Bandwidth, on the other hand, is measured in an ideal condition. It is the amount of data that can flow out in normal conditions.

# Speed

- Is determined by the network adapter's configuration
- Can be impacted by the slow network devices, such as a switch



The network devices have Ethernet ports that have a specific speed. If you check the network adapter properties in your system, a specific duplex mode is selected that determines its speed. When a device has to communicate with another device, both should have the same speed configured. For example, you will likely face issues if you have a hub that operates at 10 Mbps, but your system is configured at 1000 Mbps. To deal with such a scenario, the auto mode should be selected. With the auto mode, the system will match the speed of the other device to which it is communicating.

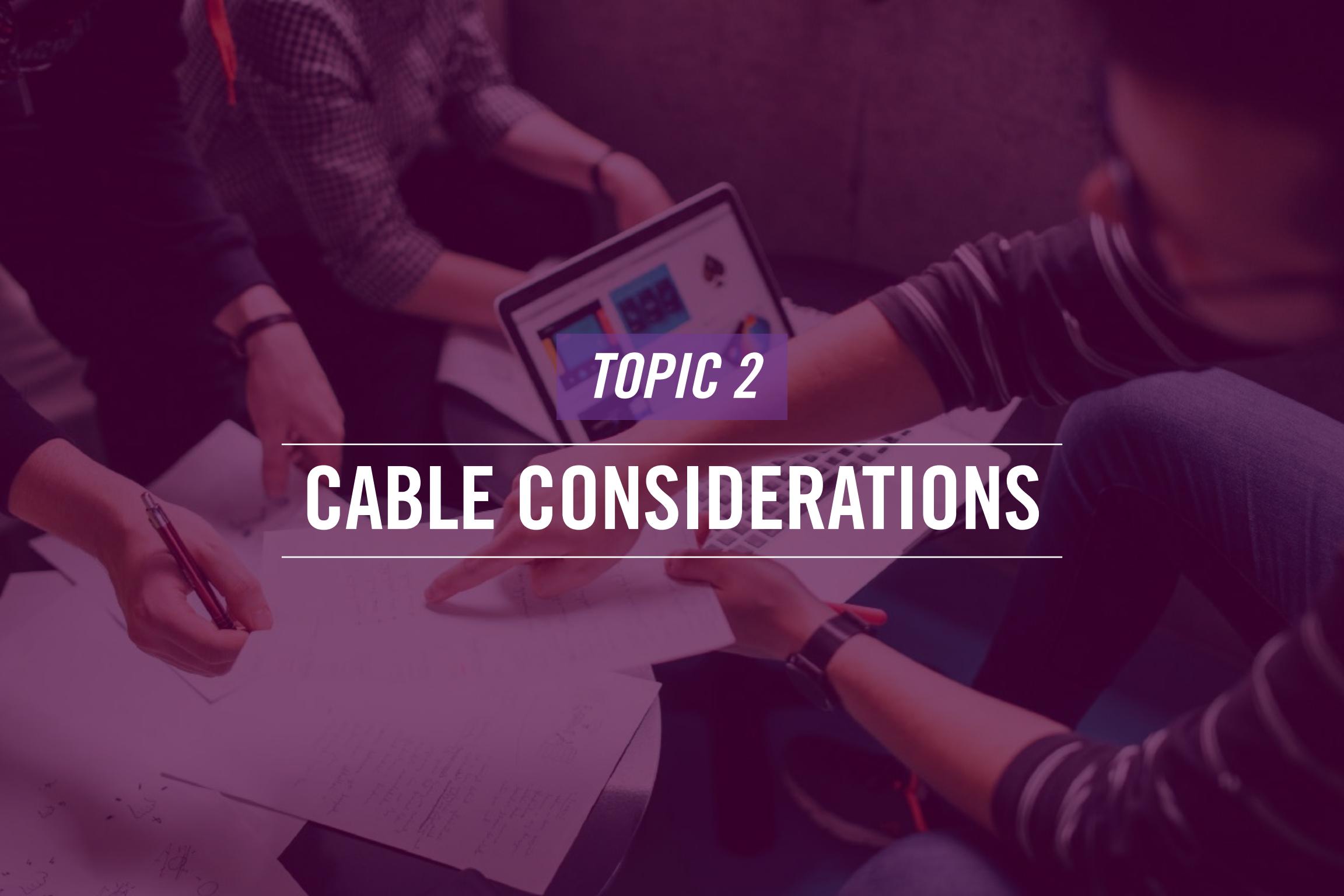
# Throughput

Features	CAT 5	CAT 6	CAT 7	CAT 8
frequency	100 MHz	250 MHz (6A 500 MHz)	600 MHz (7A 1000 MHz)	2000 MHz
distance	100m	100m	100m	30m
place of use	private homes	public networks	private or professional use	professional use only

Each Ethernet cable works with a specific length. In many cases, the length of the cable is ignored when troubleshooting a network problem. When the data has to travel far beyond the cable's capability, it may never reach its destination.

It is important to note that the longer distance the data needs to travel, the higher the attenuation. Therefore, the cable distance should be within the specified range. If you need to extend the transmissions, you should install a repeater, which will receive the signal at the other end of the cable and then amplify it and send it forward. This will reduce the network transmission problems.

The CAT 5, 6, and 7 cables can work with the 100-meter range. However, CAT 8 has a reduced limit of 30 meters.

A photograph showing several people's hands and arms working together on a table. One person in the center-left is holding a white tablet displaying a grid of colorful icons. Other hands are visible, some holding papers and a calculator, suggesting a collaborative work environment.

## TOPIC 2

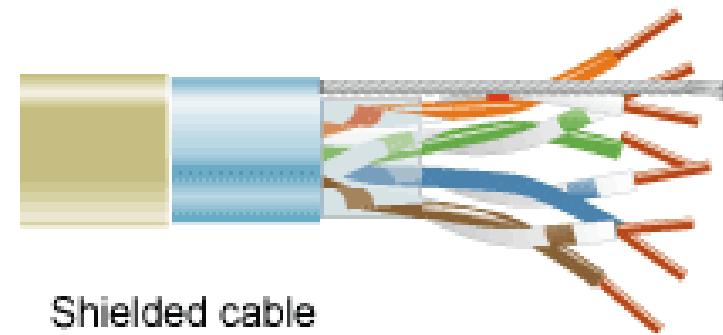
---

# CABLE CONSIDERATIONS

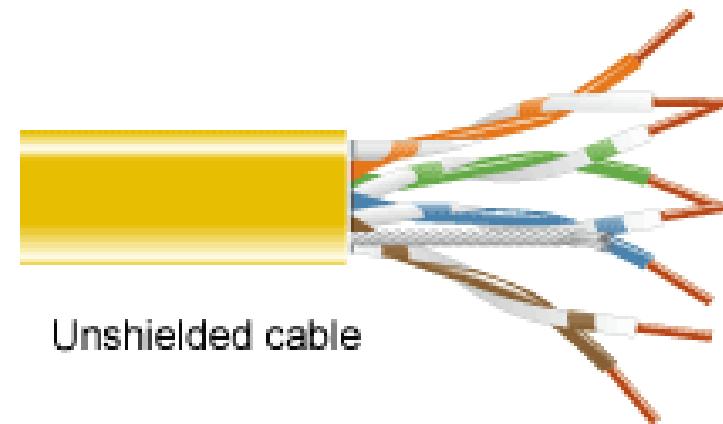
---

# Shielded and Unshielded

- Twisted:
  - Total of eight wires
    - Four sets of two cables
    - Two cables twisted around each other
- Shielded Twisted:
  - Each pair is insulated in foil
- Unshielded:
  - Each pair is not shielded



Shielded cable



Unshielded cable

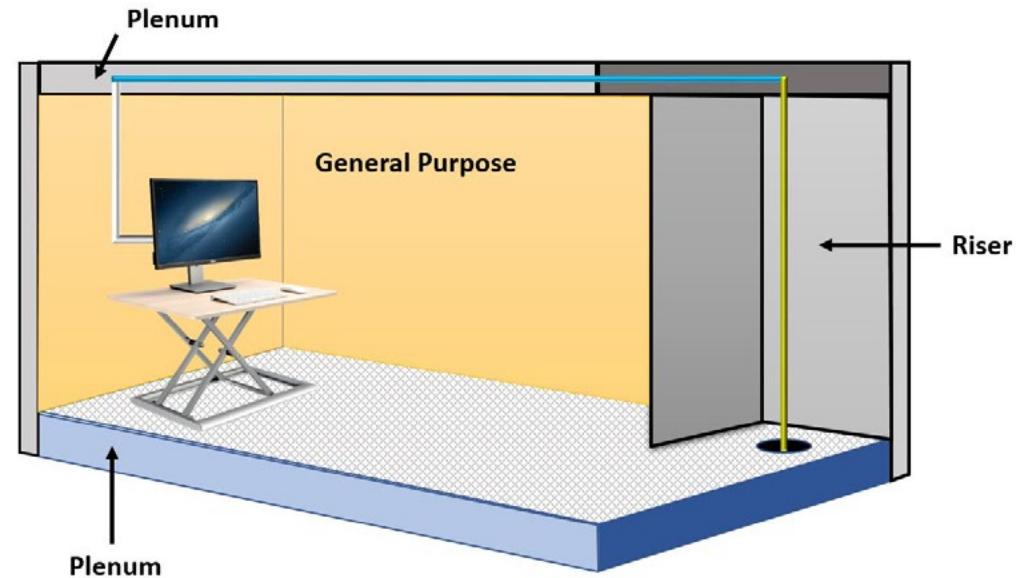
Both shielded and unshielded cables are twisted pair cables. It is called a twisted pair cable because eight wires are inside the plastic sheath. These eight wires are then divided into four pairs – two cables each. Each pair is twisted – having both the cables twisted around each other.

Let's now talk about Shielded Twisted Pair or STP is what it is known as. The four pairs jointly are in the plastic sheath, and then each pair has a separate foil coating, which is there to prevent electromagnetic interferences.

Then comes the Unshielded Twisted Pair or UTP. Functionality-wise is the same as the STP cable. It also has four pairs of two wires each. However, the fundamental difference is that the pairs are not held inside the foil. It just has a plastic sheath surrounding the eight cables or four pairs of cables. Telephone cable is an example.

# Plenum and Riser-rated

- Plenum Cables:
  - Are laid down in plenum
  - Use a cable jacket with low-toxicity material, such as Teflon or Kynar
- Riser-rated Cables
  - Have the self-extinguish capability
  - Are laid down in the non-plenum areas, such as elevator shafts



**Plenum:** Building spaces above a drop ceiling or below raised floors used for air flow or air distribution systems

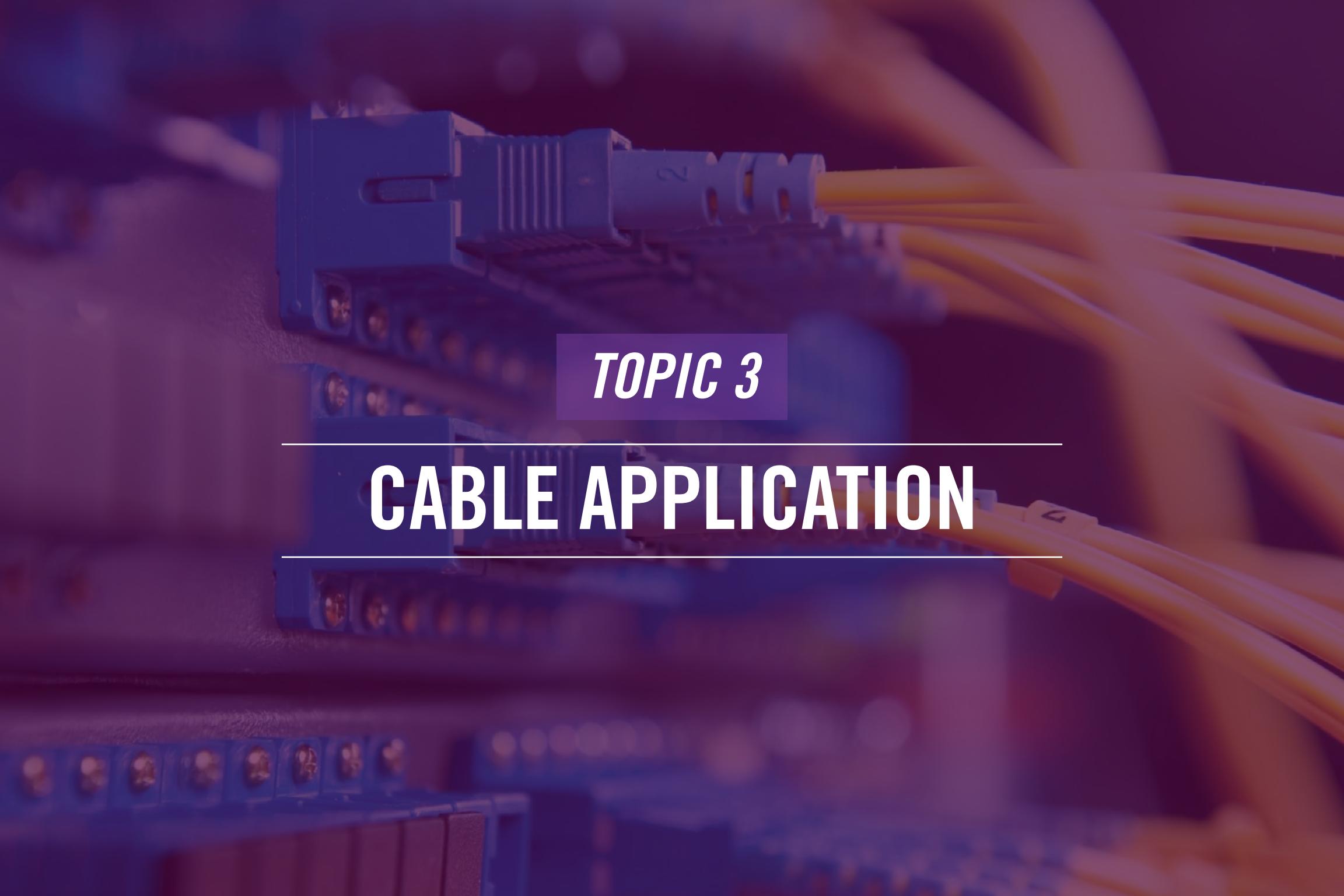
**Riser:** Building area such as shafts or ducts that run vertically through one or more floors

**General Purpose:** All other areas that are not plenum or riser and on the same floor

As you might have guessed, the plenum cables are designed to be laid down in the plenum, which is the space between the ceiling tiles and the roof. In most cases, the plenum is used for air conditioning ducts. You lay down the plenum cables in this space. The plenum cables use a cable jacket with low-toxicity material, such as Teflon or Kynar. They are fire-resistant and do not produce toxic material.

The riser-rated cables can prevent the fire from spreading vertically using its self-extinguish capability. You cannot use riser cables as a replacement for plenum cables. However, you can use plenum cables to replace the riser cable.

The riser cables are used where you cannot use the plenum cables. Two examples are cable risers and elevator shafts.



## *TOPIC 3*

---

# CABLE APPLICATION

---

# Rollover Cable/Console Cable

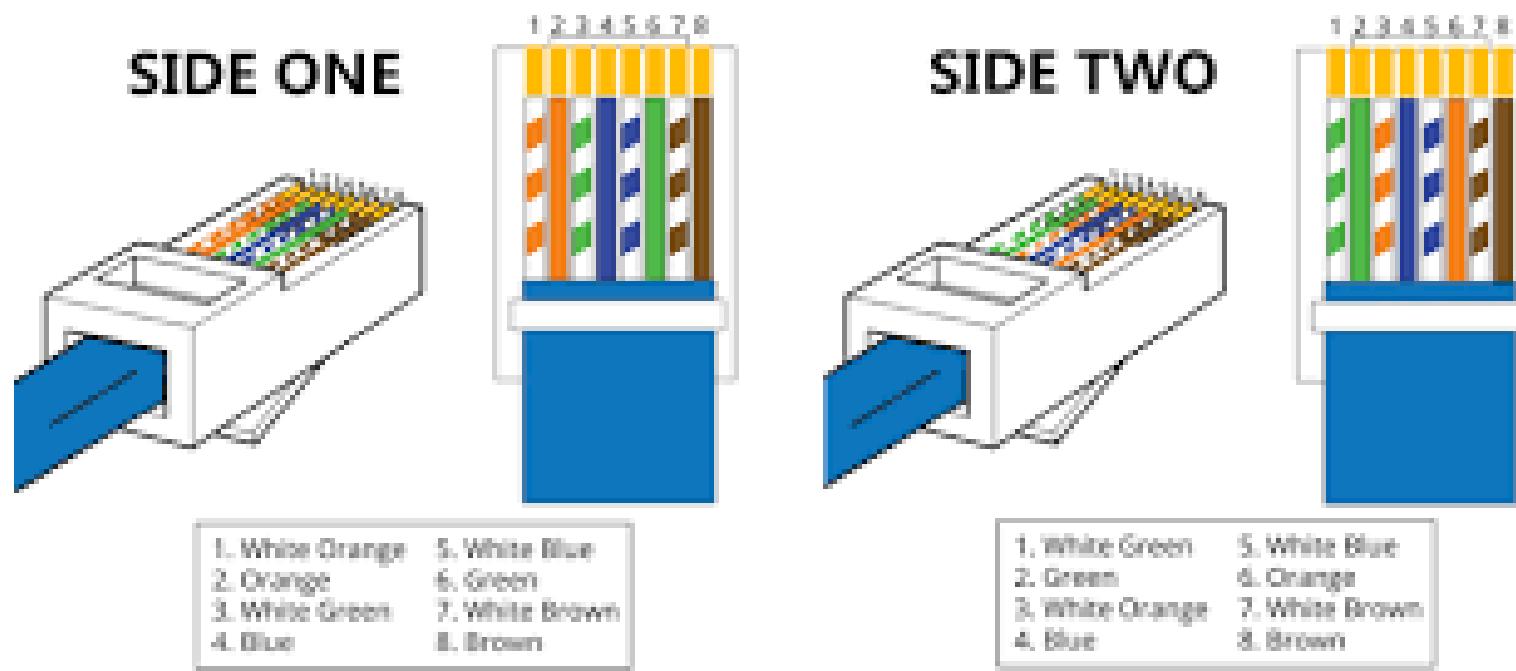
- Has one end as RJ45 and another end with DB9 connectors



A rollover is a less famous name for a console cable, with two different connectors at each end. You have the RJ45 connector on one end, which is a male. On the other end, you have a DB9 female connector. Unlike the other networking cables, the console cable is typically a flat blue cable with connectors at both ends.

The console cable is used for the initial configuration of the networking devices, such as a router or a switch with a serial port. The DB9 port is connected to the serial port on the device, and the other end with the RJ45 connector is connected to the system.

# Crossover Cable



In most cases, you will connect a system to a network and communicate with the other systems. However, you often need to directly connect a system to another system or even switch to another switch for cascading purposes. You need to use a crossover cable for this purpose.

A crossover cable is an Ethernet cable with two male RJ45 connectors – one at each end. This is the typical physical appearance of an Ethernet cable. However, one connector contains the eight cables in a typical order, but the other has a few cables switched. There are technical names for both ends of the crossover cable. One end is known as T-568A that has the cables in the following order:

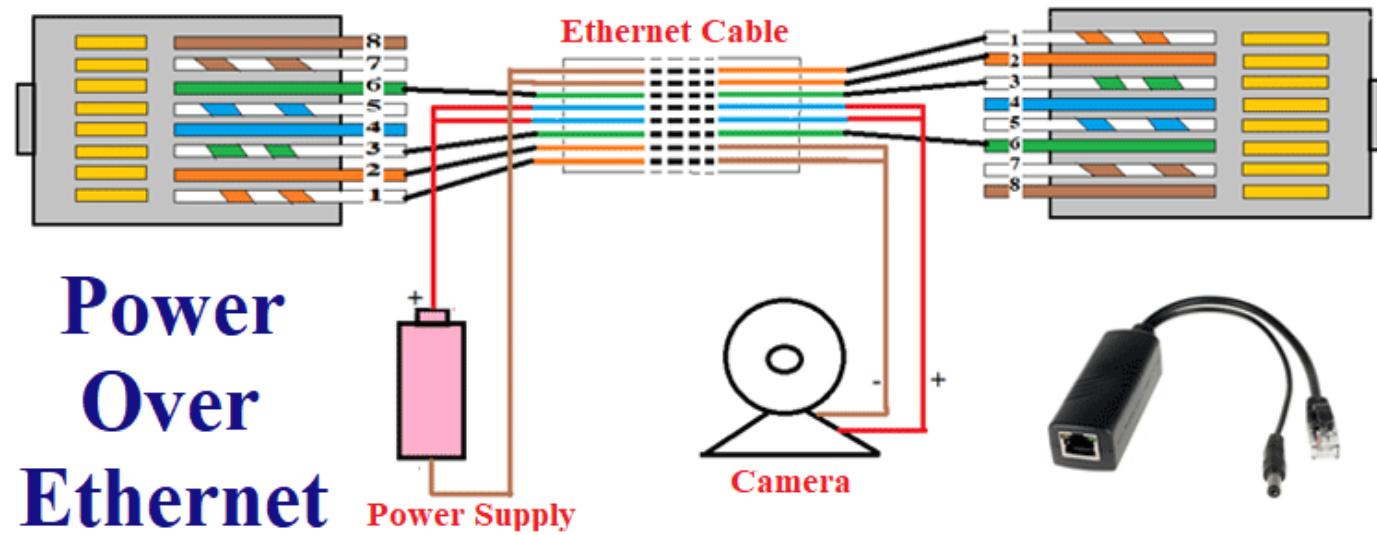
- White Green • Green • White Orange • Blue • White Blue • Orange • White Brown • Brown

The other end of the crossover cable is known as T-568B. It contains the cables in the following order:

- White Orange • Orange • White Green • Blue • White Blue • Green • White Brown • Brown

# Power over Ethernet

- Is an 802.3af IEEE standard
- Provides power to various networking devices using the Ethernet cable
- Uses the same cable for data and power



Power over Ethernet (PoE) is an 802.3af IEEE standard that allows several networking devices to be powered on using the Ethernet cable. You may have to install a network device, like a wireless access point, in a location where there is no power available. You can use PoE to power on the wireless access point in such a case. Typically, an Ethernet cable is used for data transmission and network connectivity. However, the power is also provided to the network device with the PoE, and the data transmission takes place on the same cable. PoE is now available in two different variants:

- 802.3af: Is PoE that can provide 15.4 watts of power
- 802.3at: Is PoE+ that can provide 25.5 watts of power

The devices need to be PoE or PoE+ enabled.

## *TOPIC 4*

---

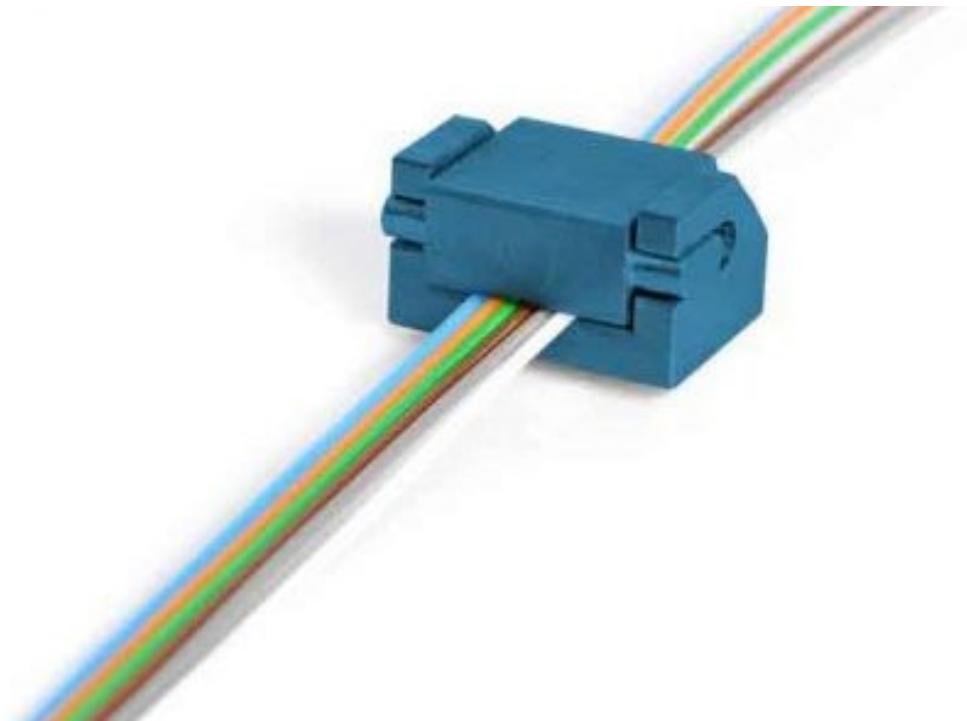
# COMMON ISSUES

---



# Attenuation

- Occurs in cables due to joins and splices
- Causes issues in fiber-optic cables
  - More splices – more attenuation

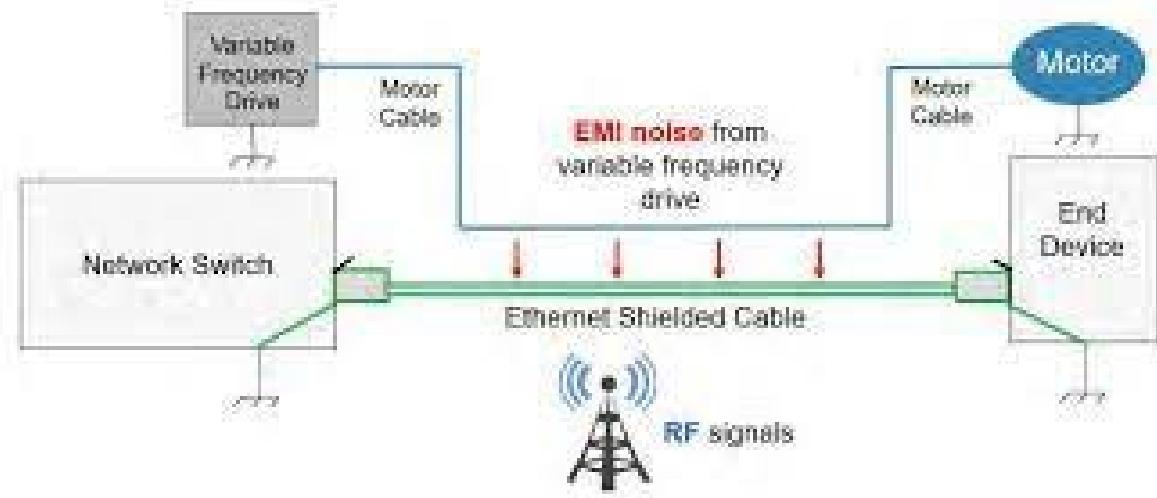


Even though fiber-optic does not suffer from high attenuation, it can occur if there are splices and joins in the fiber. The more splices and joins you have in fiber, the higher the attenuation. You can use an oscilloscope or toner probe to detect attenuation in fiber optic cables.

UTP cables are prone to attenuation. STP cables are less prone to attenuation, but they still suffer from attenuation. Longer cable lengths generate more attenuation. To prevent attenuation in twisted pair cables, it is advisable to use repeaters.

# Interference

- Occurs mainly due to electrical devices:
  - Heavy machinery
  - Cordless phone
  - Microwave
  - Power cables
  - Electrical motors



Interference is the disturbance caused by the Ethernet cables. Interference occurs due to various external devices or components, such as:

- fluorescent lights
- Heavy machinery
- Cordless phone
- Microwave
- Power cables
- Electrical motors

Interference affects data transmission. Depending on the type of cable you use, the interference may not affect the transmission. For example, UTP cable is prone to interference. On the other hand, fiber optic is resistant to interference from electrical devices like power cables or microwaves.

To reduce the interference, you need to ensure that the cables are laid down away from the monitors, microwaves, and any device that creates electromagnetic interferences.

# Decibel (dB) Loss

- Occurs due to the increased attenuation
  - Attenuation is measured in decibels
  - Attenuation is also known as dB loss
- Is mainly present in the copper cables

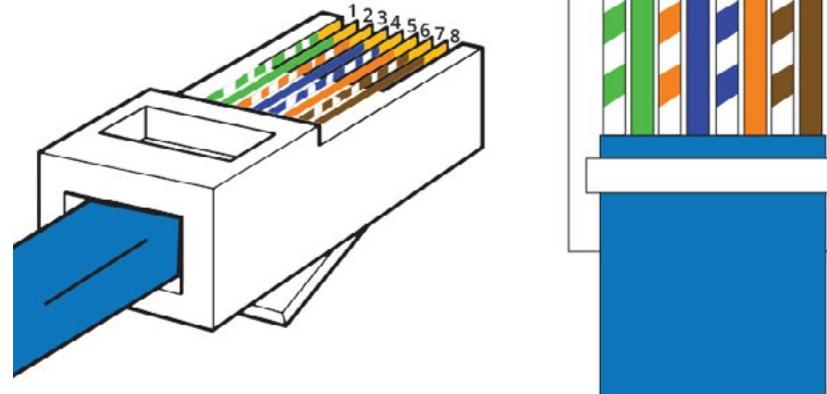


You have already learned about attenuation. Decibel loss is the other name for it. There is higher decibel loss when there is high attenuation, which is there in the twisted pair cables. UTP is more prone than STP cables.

When a transmission is sent on a wire, as the data moves away from the source, the attenuation increases, which eventually increases the decibel loss.

# Incorrect Pinout

## RJ45 Pinout T-568A

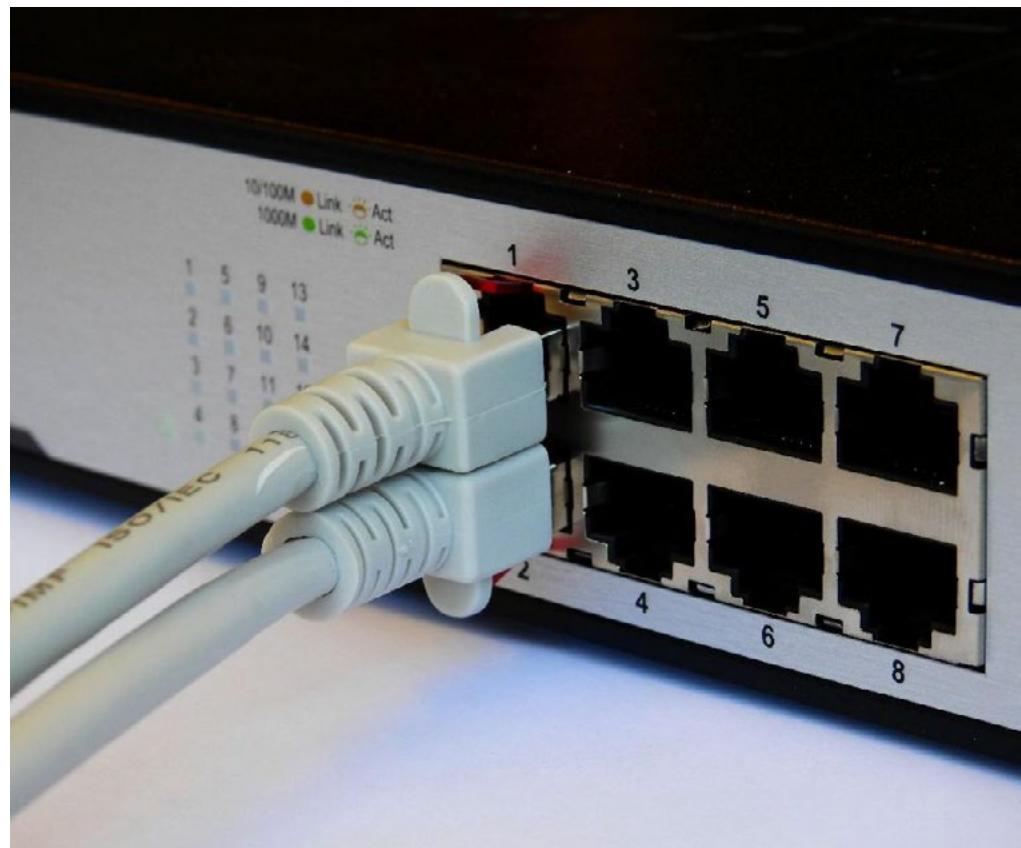


The cables within the Ethernet cable need to be plugged into the RJ45 connector in a specific order. This is called the pinout order. If the cables are not put in the correct order, the Ethernet cable does not work.



# Bad Ports

- Has one end as RJ45 and another end with DB9 connectors



The RJ45 connects to the ports – it could be a network adapter, switch port, or even a router. When you connect a cable to a port on a network adapter, and the other end is connected to a switch, the lights on the ports would light up, typically a green light. If the lights don't light up, you may want to check the cable first. If the cable is working, you can suspect that either the network adapter port or the switch port is gone bad. To confirm this doubt, you may want to connect another system or device on the same port to see whether it is functional.

# Open/Short

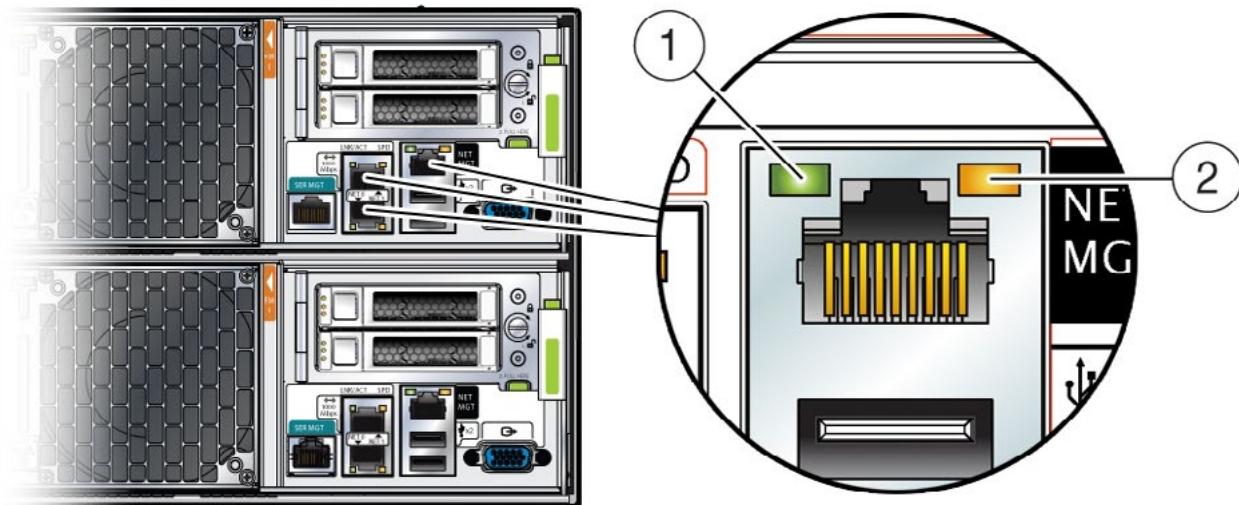
- Open:
  - Cable is broken or cut
- Short:
  - Data travels to the wrong wires
  - Two cables have cuts and cuts are being touched



A cable can have different physical faults – known as open/short. An open fault occurs when the cable is broken or cut into two pieces. The short fault occurs when the cable's insulation has come off or is torn, and internal metal wiring is touching another cable that has broken insulation. In this case, both the cables' internal metal wires are touching each other, which creates a short fault. In both cases, the cables are non-functional. A critical Ethernet cable, such as a network backbone, could lead to network downtime. You can use a cable analyzer to detect such faults and replace the cable(s).

# Light-emitting Diode (LED) Status Indicators

- Are indicators on the network adapter or network interface card
- Are usually in two colors: green and orange
- Are also found on all network devices that have network ports

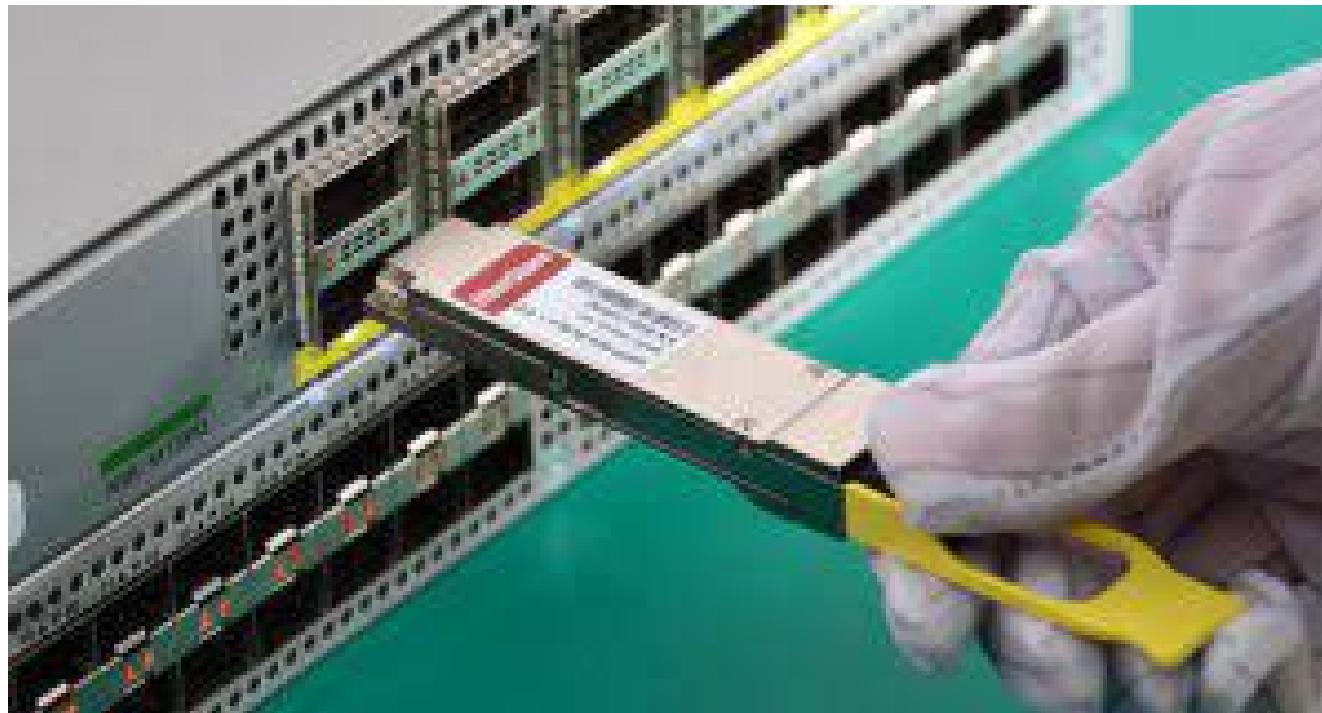


As stated earlier, each network port has light indicators. When you connect a cable to a port and the other end of the cable is connected to a switch or another device, the light indicator of the port lights up. Each port typically has two LED indicators – green and orange. When it lights up, the green one indicates that the port is working. The orange one typically indicates a problem.

The LED indicators are found on all networking devices that have ports. For example, you will find them on the switches, routers, and network adapters.

# Incorrect Transceivers

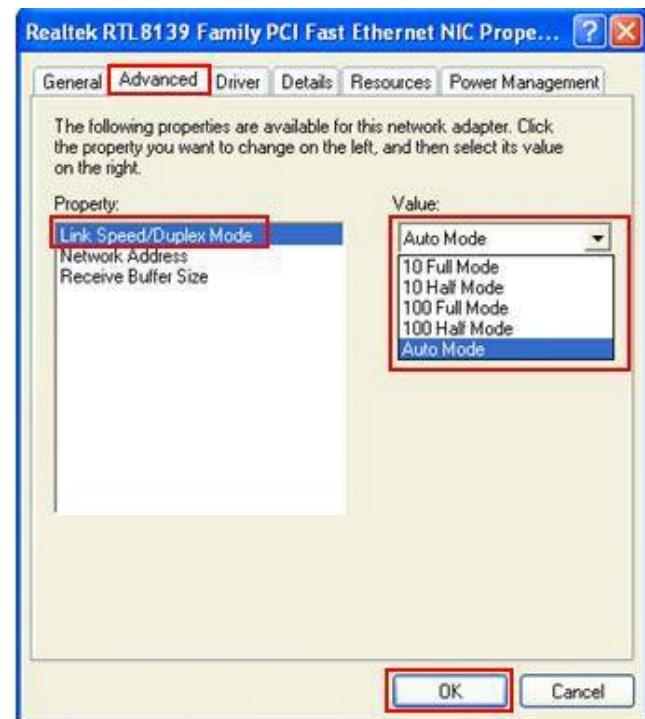
- Can be the cause of broken or no connectivity



An incorrect or mismatched transceiver can be the cause of connectivity. For example, you need to use a single-mode fiber transceiver with the single-mode fiber. Similarly, you need to use a multimode fiber transceiver with the multimode interface. It is necessary that you must use the correct transceivers at both ends to ensure proper connectivity.

# Duplexing Issues

- Occur when the network duplex modes are different between two devices
- Results in packet losses
- Can be resolved by setting both the devices with the same duplex mode



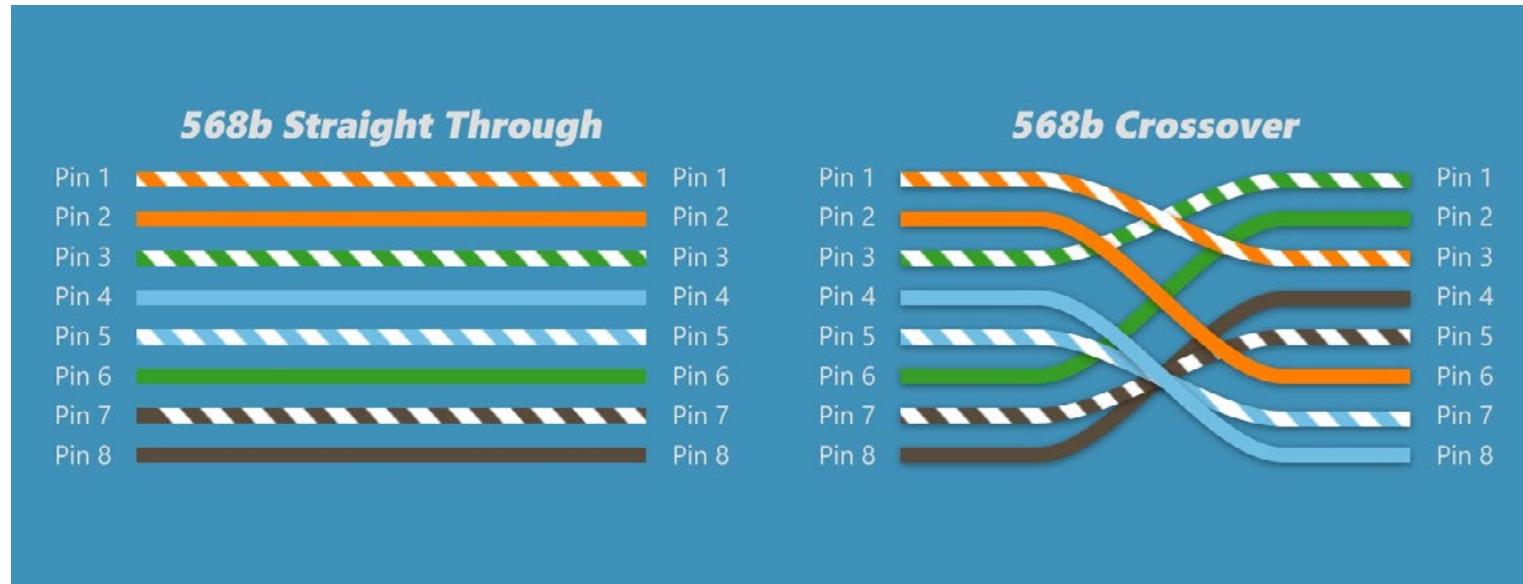
[Changing the Speed and Duplex Mode of Network Card in Microsoft Windows \(home-network-help.com\)](#)

Two devices on a network need to communicate using the same mode. Each network adapter or a network device has a specific speed defined. For example, you must have heard or read about a 1 Gbps network adapter or a switch. This is the maximum speed at which they can operate. However, the other end of the communication, let's say a switch, may not communicate at the same speed. This can lead to packet loss. If the system sends out data with 1 Gbps speed but the switch can process only at 100 Mbps, there will be packet loss.

It is possible to configure the speed in most cases. For example, in Windows, you can set the network adapter speeds. You can set it to Full or Half-duplex.

# Transmit and Receive (TX/RX) Reversed

- Is done in a crossover cable by reversing the TX and RX cables
- Is done to connect two similar devices
  - Two systems
  - Two switches



The TX and RX are reversed in a crossover cable. The straight Ethernet cable has wires in a specific order. However, in the crossover cable, the order of the cables is changed. This is required to connect two similar devices. For example, if you do not have a switch but need to form a small network by connecting two systems, you will need a crossover cable. Similarly, you will need to use the crossover cable when connecting two switches.

# Dirty Optical Cables

- Can cause various issues, such as:
  - Fiber network failure
  - Fiber cable failure
  - Intermittent packet losses
- Can be cleaned using specialized kits available



If you are facing connectivity losses on a fiber network, you might want to check for the broken fiber cables. If you do not find any broken fiber cable, then you need to check for the dirty fiber cables, which can cause:

- Fiber network failure
- Fiber cable failure
- Intermittent packet losses

The fiber cable connectors can accumulate dust and need to be cleaned from time to time. There are ready-made fiber cleaning kits available in the market that you can use. In a kit, you would typically have:

- Isopropyl alcohol
- Micro dust spray
- Fiber optic wipes
- Microscope for checking the dust inside the connector
- Dry woven cloth



## *TOPIC 5*

---

# COMMON TOOLS

---

# Cable Crimper



In most cases, you will use a factory-made Ethernet cable with connectors at both ends. However, you may need to prepare an Ethernet cable or even create a crossover cable in some situations. To do that, you need to crimp the RJ45 connectors at both ends. Crimping the RJ45 connectors requires a crimping tool known as a cable crimper or a wire crimper.

With the crimping tool, you can connect the connectors at the end of the cable. You need to insert the cables inside the connector and place the connector in the crimping tool. When you press both the handles, the connector tightly crimps the cables in their respective places.

Other than RJ45, you can also crimp the telephone wires with the RJ11 connectors.

As a side note, the technical name for the RJ45 connector is 8P8C. Similarly, the technical name for RJ11 is 6P4C.

# Punchdown Tool



In the server room or data centers, you will have patch panels, which are the termination points for all the cables that have been laid down. All these cables need to be punched into the back of the patch panel. In the front of the patch panel, the one end of the cables with RJ45 connectors are connected. The other ends of the cables are connected to the switches.

It is impossible to terminate the cables in the back of the patch panel with bare hands. You need to use the punchdown tool. You put the cable to the point where it needs to be terminated and then press the punchdown tool. It removes the insulation from the cable and pushes the cable into the point, which is a connector.

# Tone Generator



[711K-G Tempo | Tempo 711K-G Tone Generator, 3 Tone | 196-8355 | RS Components \(rsdelivers.com\)](#)

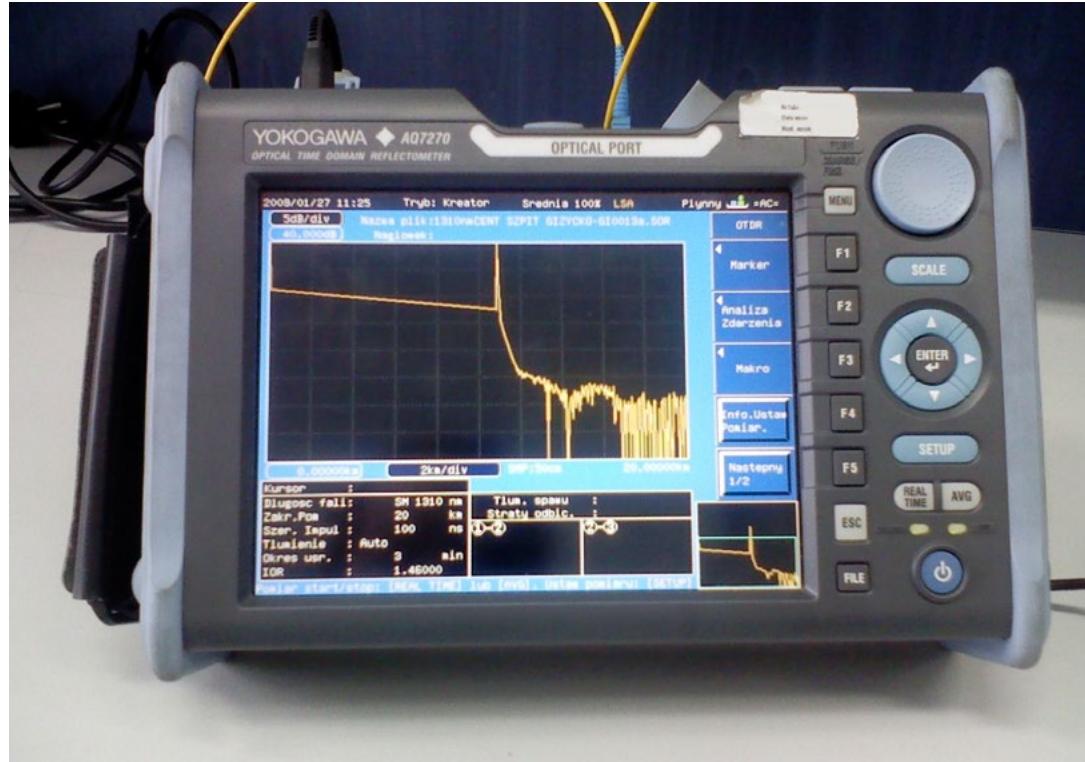
A tone generator is a UTP cable testing tool. You need to put one end of the cable into the tone generator—the other end of the UTP cable is put into the tone locator. The tone generator sends a signal via the cable. If the signal reaches the other end, which is in the tone locator, it beeps. This means that the UTP cable is in working condition. The primary use of the tone generator is to test the cables. You can also use it to locate faults within the cables.

# Loopback Adapter



A lookback adaptor is used to troubleshoot network transmissions. It works simply. If you suspect there is a problem with a port, you connect the loopback adapter on the port. It then generates transmission signals that should be received by the receiving point, which is usually a switch. When a switch is at the receiving end, its respective port lights will light up. This means that the port is in working condition.

# Optical-time Domain Reflectometer (OTDR)



An optical time-domain reflectometer (OTDR) is a fiber cable testing device. It transmits optical pulses over the fiber cable to determine an issue. Using OTDR, you can perform the following tests with the fiber cable:

- Determine the length of the fiber cable
- Locate the faults and determine their locations
- Locate any breakage in the fiber cable and location of the breakage
- Malfunctioning or bad connectors
- Any bends in the fiber cable

# Multimeter



You must have seen a lot of electricians carrying a multimeter. Electricians use a common device to measure voltage, current, or resistance. Multimeters are also used in the networking world. They are used to generate the ping responses from the networking devices. They can be used to locate cable faults. You can also use multimeters to locate cables on the patch panels.

A multimeter is equipped with two probes, red and black. The probes are touched on a conductor, and the results are shown on the multimeter.

You have two types of multimeters:

- Analog: It uses a needle to show the measurement.
- Digital: It uses a numeric digital display.

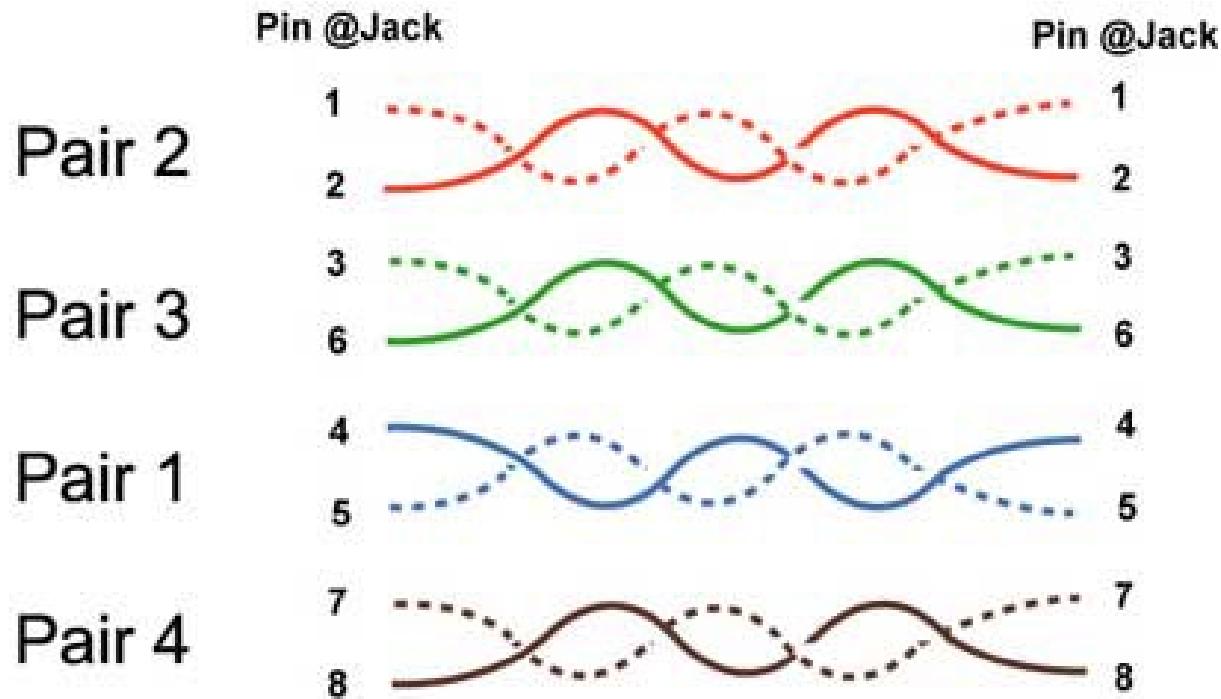
# Cable Tester



A cable tester is used to test the Ethernet cables. It can also test the telephone cables with the RJ11 connectors. A cable tester, also known as a media tester, has two components. The first is a battery-powered active component that generates and sends signals to the connected wire. The other end of the wire is connected to the passive component, receiving the signals. The core intent of using a cable tester is to test whether an Ethernet or telephone cable is working properly or not. It can also help you verify the connectors and faults on the cable.

# Wire Map

Wiremap For T568B\*



\*T568A reverses orange & green pairs

Wire map or wiremap is a test to verify the Ethernet cable connectivity. It is performed to locate the opens, shorts, or reversed wires if there are any. Using wiremap, the tester sends out signals on each cable inside the Ethernet cable. It then can detect if there are faults with the cable.

# Tap



A tap, more commonly known as network tap, is used to replicate the traffic transmitted on a network. It does not alter the traffic and is a non-intrusive device. It makes a copy of the network traffic for various reasons, such as:

- Network monitoring and analysis: This can be helpful if you are dealing with bandwidth saturation and latency. With the copy of the traffic, you can leave the real-time traffic untouched but analyze its copy.
- Malicious traffic detection: You can filter the copy of the traffic to find any malicious or intrusive traffic.

There may be various other use cases for network traffic, depending on the situation. Network traffic can be plugged into a network in different locations, but it depends on the type of network architecture.

# Fusion Splicer



A fusion splicer is used to join two pieces of a fiber cable or two fiber cables as one. Sometimes, a fiber cable is broken due to whatever reason. To connect the broken fiber cable, you can use a fusion splicer. You have to keep both the broken ends in the fusion splicer. It uses the electric arc to melt both the ends and join them as a single fiber cable. The process is quick and gets completed in less than a minute.

# Spectrum Analyzer



A spectrum analyzer is used to measure different signals, such as electrical, acoustic pressure waves, and optical light waves. Spectrum analyzers are used for troubleshooting signal problems. They are mainly used with the wireless networks to:

- Detect the 2.4 and 5.0 GHz frequencies
- Detect hotspots
- Detect wireless networks

# Snips/Cutters



Snips, also known as cutters, are used for cutting the wires. In general, snips are tools that are used for cutting metal sheets. Visually, they look like a scissor but are larger in size, ranging from 7 to 14 inches. There are two types of snips:

Snips are used for cutting wires. For example, if you buy a large bundle of Ethernet cables, you need to cut the single long wire into several pieces.

# Cable Stripper



Remember, an Ethernet cable has four pairs of cables that are protected with a protective coating, which is also known as rubber insulation. If you need to put a connector on one end, you need to remove the protective coating. To do this, you can use a cable stripper. A cable or wire stripper removes the protective coating from the Ethernet cable. You need to put the cable in the correct slot and close its mouth by inward pressing both handles. It is important to note that a cable stripper can be used with different types of cables, and therefore, you need to be sure that you choose the correct slot.

# Fiber Light Meter



A fiber-optic light meter, also known as an Optical Power Meter (OPM), measures the movement of light in the fiber optic cable. It is used to measure the optical signal loss through the fiber cable. You need to connect one end to the light source and the other end to the meter, displaying the results.

# Summary

- Specifications and limitations
- Cable considerations
- Cable application
- Common issues
- Common tools



That's the end of the lesson.

Here we covered:

- Specifications and limitations
- Cable considerations
- Cable application
- Common issues
- Common tools



**NEXT TOPIC**

---

# NETWORK TOOLS AND COMMANDS

---



# 3

---

# Network Tools & Commands

- 1 — Welcome to the 3 lesson of Module 5. In this lesson, you will learn about the:
  - 2 — Network Tools and Commands
-

# Agenda

- Software tools
- Command line tool
- Basic network platform commands



Hi, welcome to COMPTIA Network+ Course

In this lesson, we will talk about:

- Software tools
- Command line tool
- Basic network platform commands



## *TOPIC 1*

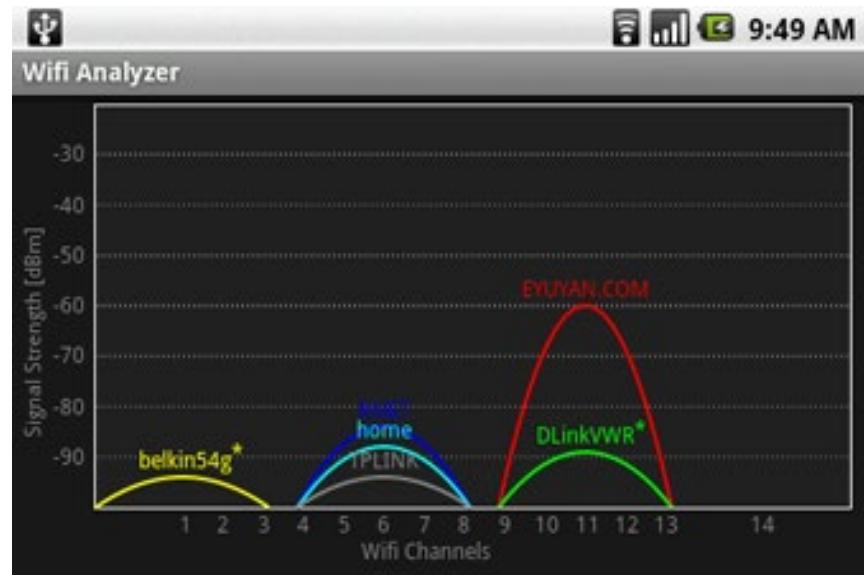
---

# SOFTWARE TOOLS

---

# WiFi analyzer

- Are used to map the entire site
- Are used to identify interference and the blind spots
- Can help to determine the speed
- Help you determine the appropriate configuration



When installing a wireless network, you need to be extremely cautious about interferences, blind spots, and so on. You need to ensure optimal signal strength reaching the users when you set up the wireless access points (WAPs). With the help of a wireless or WiFi analyzer, you can map the entire site and determine quite a few key things like:

- Data transmission rates
- Maximum supported speeds
- Network coverage
- Interferences
- Blind spots

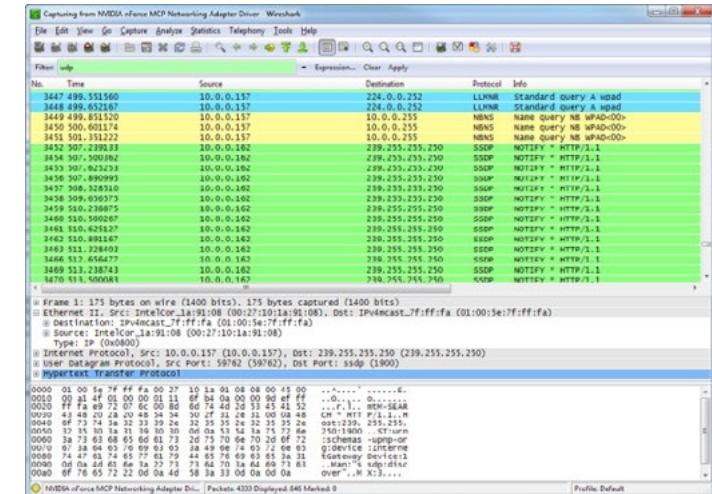
In short, WiFi analyzers are a key tool for inspecting your site to place the WAPs and determine the number of WAPs required. However, even after you have implemented the wireless network, you can still use the WiFi analyzers to determine:

- The assets on the wireless network
- Their MAC addresses
- Speed of the wireless network
- Requirement for any additional WAPs

With the help of the WiFi analyzer, you can also test and determine the correct configuration. For example, you may have to change the channel configuration as there may be a channel overlap.

# Protocol Analyzer/Packet Capture

- Can be hardware or software-based
- Help to analyze the network protocols
- Are mainly used to troubleshoot network protocols by capturing and decoding the communication
- Can track the bandwidth used by a protocol



Protocol analyzers are used for analyzing the protocol information over a network. There can be software or hardware-based protocol analyzers. You can capture the network traffic to analyze the information about a particular protocol. For example, if there is HTTP-based traffic, you can inspect the traffic and verify the information passed on.

There are various uses of a protocol analyzer. You can:

- Identify the type of network traffic
- Filter the traffic
- Identify the ports being used by the traffic

In most cases, the protocol analyzers are used for network monitoring and troubleshooting network problems. For example, let's look at a scenario. You have set up a small network, but the network traffic is not going to the Internet. Without a protocol analyzer, it would not be easy to interpret where the traffic is going. With the packet analyzer, you can determine the path the traffic is taking and the location it is being sent to instead of the Internet. One of the key advantages of a protocol analyzer is that it can capture and decode the network traffic, which helps a network administrator to understand the type of traffic being transmitted.

Packet analyzers can also determine the amount of bandwidth being used by a protocol.

# Bandwidth Speed Tester

- Help to determine the download and upload speed of a connection
- Can help you determine the
  - Jitters
  - Latency
  - Packet loss
- Are usually free tools provided by various organizations
- Can also be provided by an Internet Service Provider



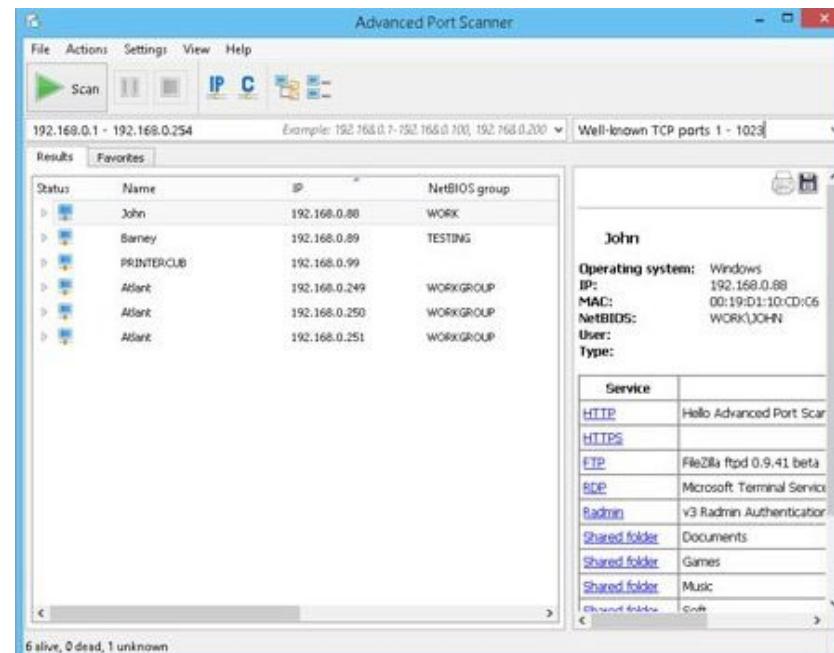
Often at home, you are troubled with the slow Internet connectivity. To resolve this, you call the Internet Service Provider or the ISP. They direct you to an online bandwidth speed testing website, which helps you determine your connection's download and upload speed. One of the key websites for speed tests is [www.speedtest.net](http://www.speedtest.net).

Depending on the bandwidth speed tester you use, you can determine quite a bit of information, such as jitter, latency, and packet loss. You can also determine the ping results in milliseconds. However, different bandwidth speed testers provide different information.

Just like [www.speedtest.net](http://www.speedtest.net), there are various other speed testing platforms available. These are provided free of cost, in most cases, by different organizations. Even ISPs may have their own online speed testing tools available or downloadable applications that the users can install on their systems.

# Port Scanner

- Is a tool to search for open ports
  - TCP
  - UDP
- Can be performed using various tools, such as:
  - TCP Port Scanner
  - Nmap
  - Netcat
  - Port Authority
  - Advanced Port Scanner
  - Network Scanner
  - NetScanTools



A port scanner is used to look for open ports on one or more systems. A port scanner looks for both the TCP and UDP ports. In most cases, you can scan a single system or an entire range of systems on the network to determine the open ports and the services that are linked with these ports.

Usually, you would not want to leave too many ports open on a system unless necessary. It is important to note that the open ports invite attackers to find a vulnerability in the associated services and exploit them. Therefore, to reduce the attack surface, it is crucial to minimize the number of open ports, which various applications, such as: can determine

- TCP Port Scanner
- Nmap
- Netcat
- Port Authority
- Advanced Port Scanner
- Network Scanner
- NetScanTools

# iperf

- Is a network performance measurement tool
- Can be used to create network baselines
- Works in the client/server mode:
  - Server on one system
  - Clients on the remaining systems
- Works on the Windows, Linux, and various other platforms

```
[ ID] Interval          Transfer     Bandwidth
[ 5]  0.00-1.00    sec  2.09 GBytes   17.9 Gbits/sec      (omitted)
[ 5]  1.00-2.00    sec  2.20 GBytes   18.9 Gbits/sec      (omitted)
[ 5]  2.00-3.00    sec  2.04 GBytes   17.5 Gbits/sec      (omitted)
[ 5]  0.00-1.00    sec  2.17 GBytes   18.6 Gbits/sec      (omitted)
[ 5]  1.00-2.00    sec  2.19 GBytes   18.8 Gbits/sec      (omitted)
[ 5]  2.00-3.00    sec  2.19 GBytes   18.8 Gbits/sec      (omitted)
[ 5]  3.00-4.00    sec  2.16 GBytes   18.6 Gbits/sec      (omitted)
[ 5]  4.00-5.00    sec  2.16 GBytes   18.5 Gbits/sec      (omitted)
[ 5]  5.00-5.04    sec  73.1 MBytes   15.2 Gbits/sec      (omitted)
-----
Test Complete. Summary Results:
[ ID] Interval          Transfer     Bandwidth     Retr
[ 5]  0.00-5.04    sec  10.8 GBytes   18.5 Gbits/sec      0      sender
[ 5]  0.00-5.04    sec  10.9 GBytes   18.6 Gbits/sec      0      receiver
CPU Utilization: local/receiver 0.1% (0.0%u/0.1%s), remote/sender 94.3% (0.8%u/9
3.5%s)
iperf 3.0.11
Linux yogesh-HP-2000-Notebook-PC 4.13.0-32-generic #35~16.04.1-Ubuntu SMP Thu Ja
n 25 10:13:43 UTC 2018 x86_64 x86_64 x86_64 GNU/Linux
-----
Server listening on 5001
```

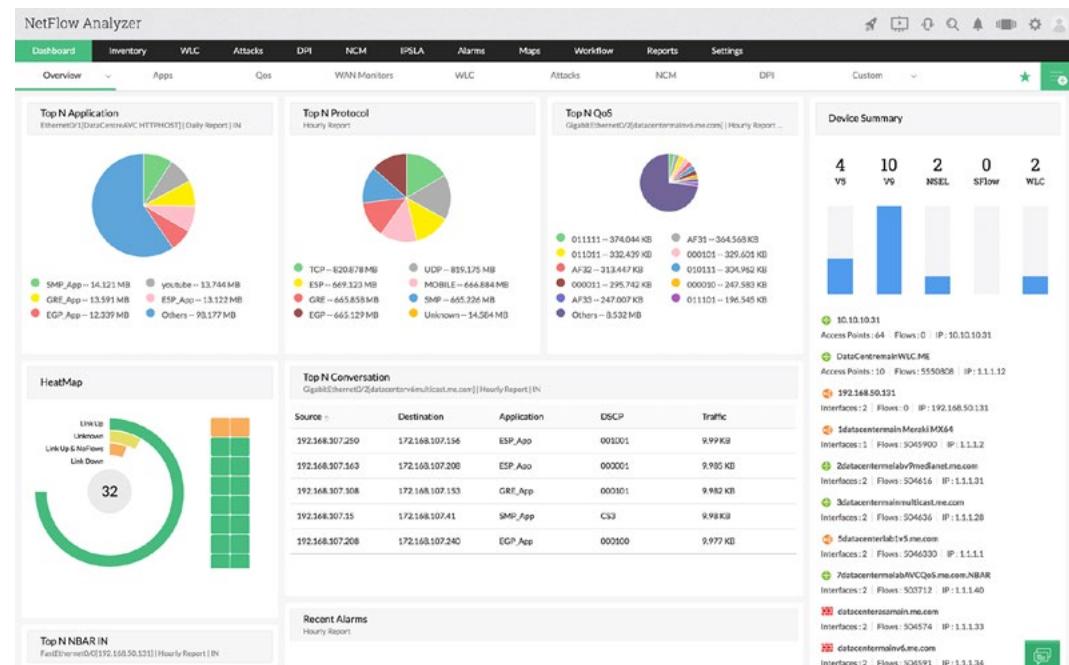
The iperf tool is an absolute necessity for network administrators who are worried about network performance. Using iperf, you can capture the network performance and create the network performance baselines. When you need to check for the network performance, you can compare it with the baseline to see if there are any issues. Based on the outcome of the comparison with the baseline, you can further tune the performance if required.

The iperf tool has a server and client component. There are options to use the public iperf servers that are listed on the iperf website.

An iperf tool is an open-source tool that works across different platforms, such as Windows and Linux.

# NetFlow Analyzers

- Is used for analyzing the application-level traffic
- Captures the incoming and outgoing traffic on a network interface
- Can be used to identify:
  - Source and destination of traffic
  - Quality of service
  - Congestion reason
- Uses port 2055



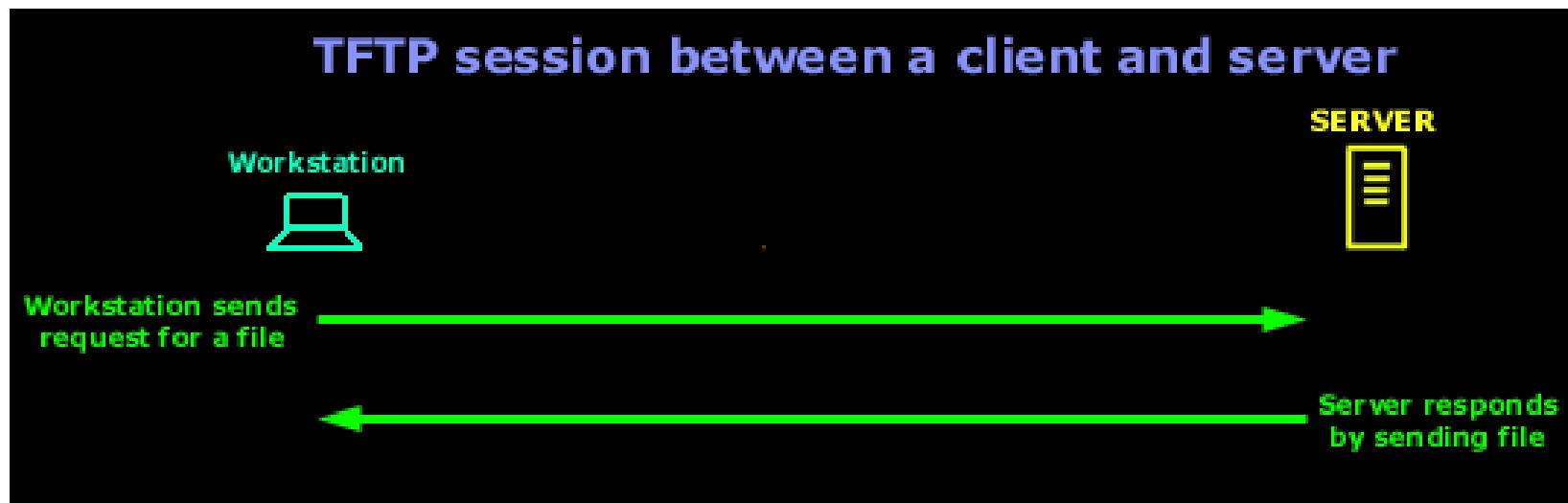
Cisco created the NetFlow protocol for network traffic analysis. With the Netflow protocol, you can use it to analyze the application-level traffic. It monitors an interface for incoming and outgoing traffic. The key intent of monitoring the traffic is to identify the following:

- Source and destination of the traffic
- Quality of service information
- Congestion reasons if there is any

The information that is generated is collected from various devices. The information can then be converted into reports for analysis. NetFlow uses port 2055.

# TFTP server

- Stands for Trivial File Transfer Protocol
- Is an open-source protocol used on various operating systems
- Is used for upgrading software on network devices
- Uses port 69



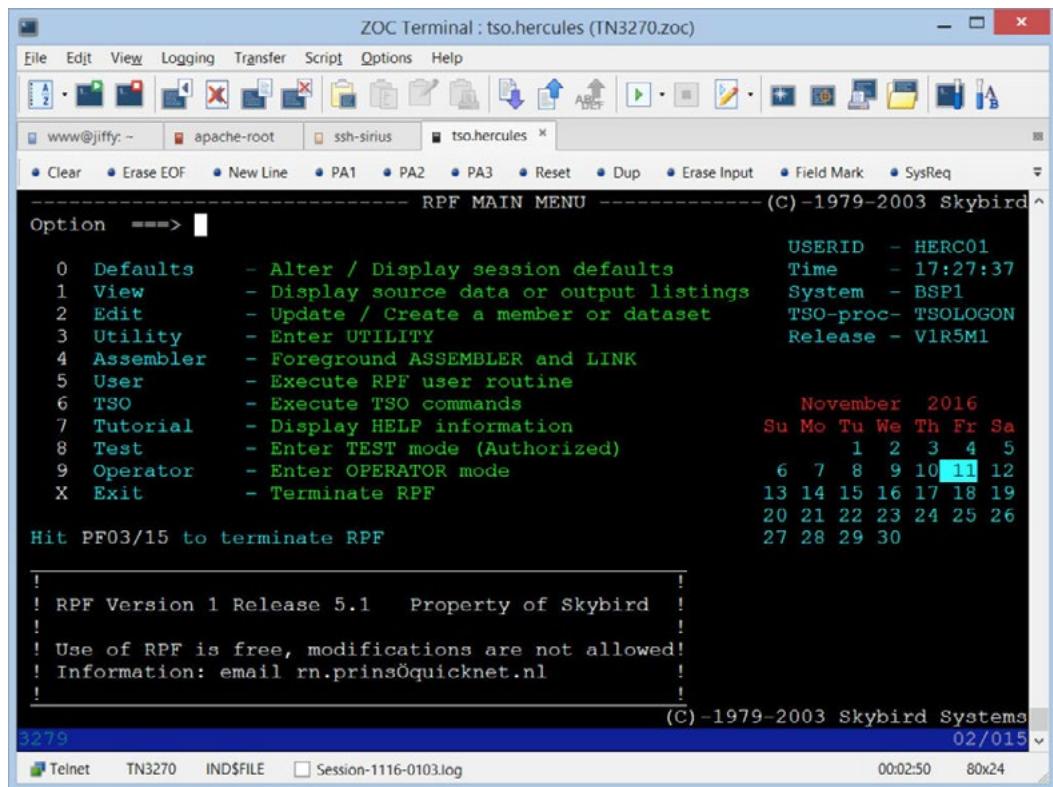
There are times when you need to update the software on a network device. This is typically done using a TFTP or Trivial File Transfer Protocol. On a system, you need to set up the TFTP server, an open-source tool, and can work across various platforms, such as Windows and Linux.

From the device, you need to specify the path to the TFTP server and the file name, and the device is then able to connect to it and download the file. This is an easy method when you need to upgrade software on the network devices.

TFTP server using port 69.

# Terminal Emulator

- Is a tool that emulates a terminal
- Is used for connecting to a remote system
- Can use protocols, such as SSH or Telnet
- Can access another system in:
  - Graphical mode
  - Command line mode
- Some examples are:
  - MobaXterm emulator
  - PuTTY
  - KiTTY



A terminal emulator, as the name suggests, emulates a terminal. Depending on the protocol for remote connectivity, you can either get the graphical or the command-line interface. For example, if you need to connect to remote Linux system, you connect to it using a tool, such Putty that can work with the SSH or Telnet protocols.

Some of the key terminal emulators are:

- MobaXterm emulator
- PuTTY
- KiTTY



# IP Scanner

- Scans for live systems on a network
  - Identifies the live IP address
  - Identifies their open ports
- Provides information about the systems:
  - Hardware information, such as manufacturer
  - MAC address
  - Software information

The screenshot shows the 'Advanced IP Scanner' application window. At the top, there's a menu bar with File, View, Settings, and Help. Below the menu is a toolbar with icons for Scan, Stop, IP, C, and Network. The main interface has a search bar with '192.168.0.90-110' and a filter field with 'hp'. The results table has columns for Status, Name, IP, Manufacturer, and MAC address. It lists five devices: NPIC9BC77, NPI1D646F, HP V1910 Switch, meeting, and Panda. The Panda entry has a 'Soft' folder expanded, showing an HP LaserJet M1522 series PCL6 Class Driver. A status message at the bottom says '5 alive, 0 dead, 0 unknown'.

Status	Name	IP	Manufacturer	MAC address
▷	NPIC9BC77	192.168.0.96	Hewlett Packard	48:0F:CF:C9:BC:77
▷	NPI1D646F	192.168.0.97	Hewlett Packard	00:1B:78:1D:64:6F
▷	HP V1910 Switch	192.168.0.102	Hewlett Packard	CC:3E:5F:5E:04:FC
▷	meeting	192.168.0.104	Edimax Technology Co. Ltd.	00:50:FC:C6:03:2B
▷	Panda	192.168.0.109	GIGA-BYTE TECHNOLOGY CO.,L...	6C:F0:49:0B:55:D5
	Soft			
	HP LaserJet M1522 series PCL6 Class Driver			

If you have a medium or large network, it is difficult for the network administrator to determine the live systems on the network. To do this, you can use an IP scanner that identifies the systems that are live on the network at the time of scanning. You can identify the live systems and their IP addresses along with the open ports on each of these systems.

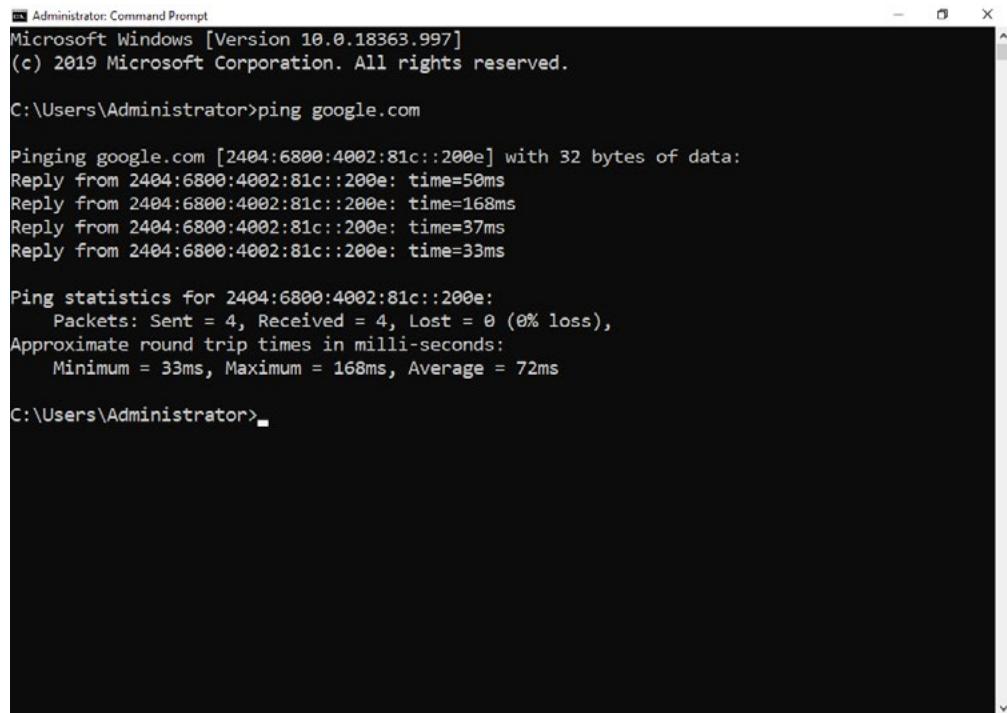
You can also determine various information, such as the manufacturer of the device, MAC address, and software information, such as the operating system. Most of the IP scanners allow you to scan a single system or a range of IP addresses.

## TOPIC 2

# COMMAND LINE TOOLS

# Ping

- Included as part of the TCP/IP stack on all operating systems
- Tests whether a host is responding or reachable on an IP network
- Can resolve IP addresses to hostnames
- Works with the hostname or IP address of the remote client
- TTL – Time To Live for a packet on the network
- ms – time taken for the data to be transmitted from source to the destination in milliseconds
- Example: ping 192.168.0.1



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.18363.997]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping google.com

Pinging google.com [2404:6800:4002:81c::200e] with 32 bytes of data:
Reply from 2404:6800:4002:81c::200e: time=50ms
Reply from 2404:6800:4002:81c::200e: time=168ms
Reply from 2404:6800:4002:81c::200e: time=37ms
Reply from 2404:6800:4002:81c::200e: time=33ms

Ping statistics for 2404:6800:4002:81c::200e:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 33ms, Maximum = 168ms, Average = 72ms

C:\Users\Administrator>
```

# Ping

In the networking world, ping is probably the very first command that you will learn. To start with, ping is included as part of the TCP/IP stack. Since all the operating systems have the TCP/IP stack, it is available on all operating systems, such as Windows, Linux, and UNIX. The key purpose of the ping tool is to check whether a host is responding or reachable on an IP network. For example, you have a Windows 10 system with the IP address: 192.168.10.10. You want to check if another system with the IP address 192.168.10.250 is reachable on the network. To do this, you need to execute the ping command:

```
ping 192.168.10.250
```

You should reply from the remote system in the following manner:

```
Reply from 192.168.10.250: bytes=32 time<10ms TTL=128
```

If the host is not reachable or responding, then you should ideally get the following error:

```
Reply from 192.168.10.250: Destination host unreachable.
```

If you type the ping command without any parameters, then the ping help is displayed. Several parameters are available for you to use. One of the key parameters is -a, which helps you resolve IP addresses to a hostname. For example, if you know the IP address of a system on the network but need to know its hostname, then you can use the -a parameter in the following way:

```
ping -a 192.168.10.250
```

It should first resolve the IP address to a hostname and then show the ping output.

When using the ping command, you can choose to use the hostname if you know it or choose to use the IP address. For example, if you have a system with the IP address 192.168.10.250, its hostname is win10-labsystem. You can use either one of them with the ping command:

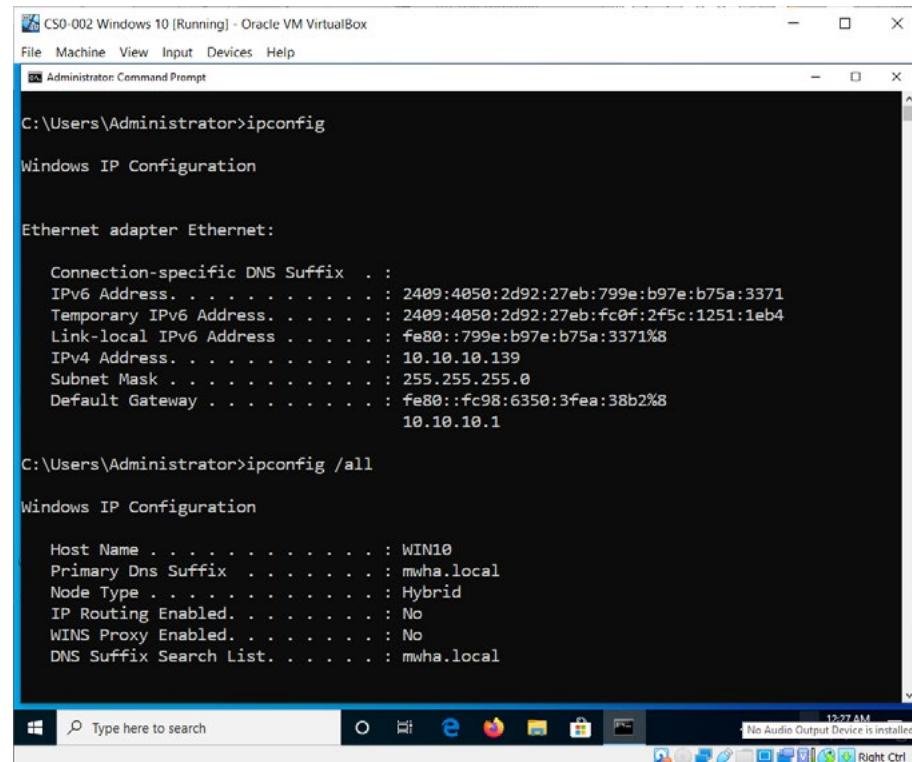
```
ping win10-labsystem  
ping 192.168.10.250
```

Both these commands generate the same output.



# ipconfig

- Is short for Internet Protocol Configuration
- Display the IP address of the local host
- Displays information including IPv4/IPv6 address, Default Gateway, and Subnet Mask
- Uses /all parameter to display additional information, including IP addresses of DNS servers
- Works on Windows systems only
- Example: ipconfig /all



```
C:\Users\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

  Connection-specific DNS Suffix . :
  IPv6 Address . . . . . : 2409:4050:2d92:27eb:799e:b97e:b75a:3371
  Temporary IPv6 Address . . . . . : 2409:4050:2d92:27eb:fc0f:2f5c:1251:1eb4
  Link-local IPv6 Address . . . . . : fe80::799e:b97e:b75a:3371%8
  IPv4 Address . . . . . : 10.10.10.139
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : fe80::fc98:6350:3fea:38b2%8
                                         10.10.10.1

C:\Users\Administrator>ipconfig /all

Windows IP Configuration

  Host Name . . . . . : WIN10
  Primary Dns Suffix . . . . . : mwha.local
  Node Type . . . . . : Hybrid
  IP Routing Enabled. . . . . : No
  WINS Proxy Enabled. . . . . : No
  DNS Suffix Search List. . . . . : mwha.local
```

Ipconfig is the short name for Internet Protocol Configuration, which is used to display the IP address of the localhost. When you run the ipconfig command, it displays the following details:

IPv4/IPv6 Address  
Subnet Mask  
Default Gateway

For example, when you execute this command, you get the following output:

```
Link-local IPv6 Address ....: fe80::6502:2a2a:6499:9860%3
IPv4 Address.....: 192.168.1.13
Subnet Mask.....: 255.255.255.0
Default Gateway..... : 192.168.1.1
```

If you need to display more information, then you need to use the /all parameter in the following manner:

```
ipconfig /all
```

You should receive the following output:

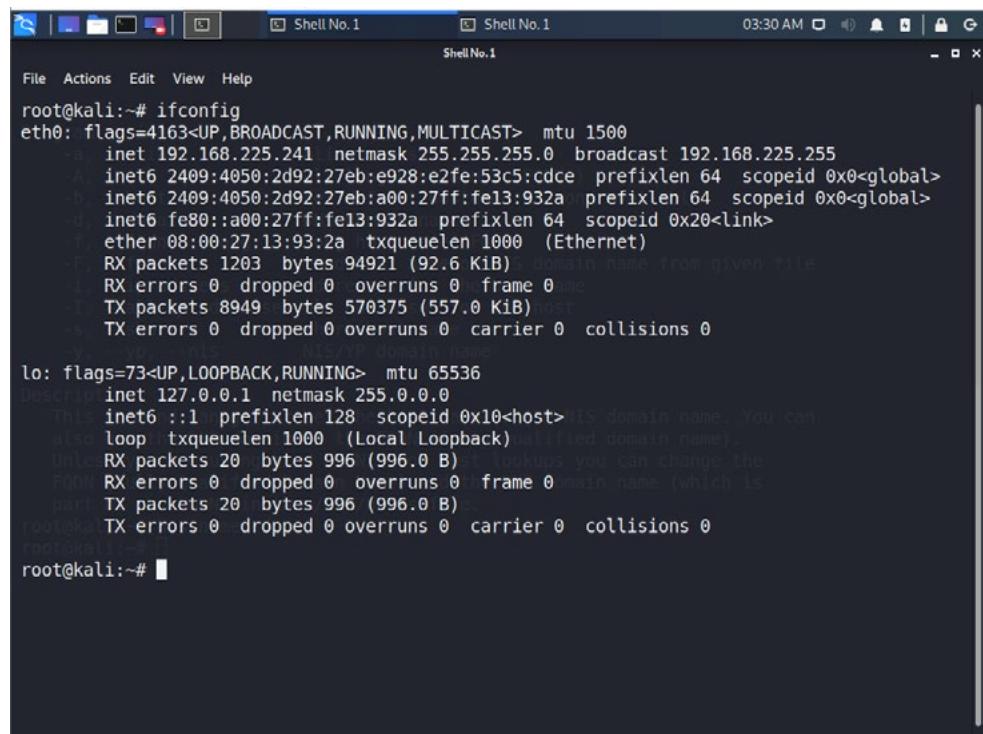
```
Connection-specific DNS Suffix .:
Description .....: Intel(R) Wireless-AC 9560 160MHz
Physical Address.....: C8-09-A8-34-70-AB
DHCP Enabled.....: Yes
Autoconfiguration Enabled....: Yes
Link-local IPv6 Address ....: fe80::6502:2a2a:6499:9860%3(Preferred)
IPv4 Address.....: 192.168.1.13(Preferred)
Subnet Mask.....: 255.255.255.0
Lease Obtained.....: Tuesday, September 21, 2021 8:35:49 AM
Lease Expires.....: Wednesday, September 22, 2021 8:35:49 AM
Default Gateway.....: 192.168.1.1
DHCP Server.....: 192.168.1.1
DHCPv6 IAID.....: 63441320
DHCPv6 Client DUID.....: 00-01-00-01-26-D6-E0-A3-C8-09-A8-34-70-AB
DNS Servers .....: 192.168.1.1
NetBIOS over Tcpip.....: Enabled
```

It is important to note that the ipconfig command works only on the Windows system. Unlike Linux or UNIX, the commands in Windows are not case-sensitive.



# ifconfig

- Works like ipconfig command on Windows
- Is short for Interface Configuration
- Displays information for all available but enabled network adapters
- Uses the –a parameter that is equivalent to /all of ipconfig
- Works on Linux and UNIX systems
- Example: ifconfig -a



```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 192.168.225.241 netmask 255.255.255.0 broadcast 192.168.225.255
            inet6 2409:4050:2d92:27eb:e928:e2fe:53c5:cdce prefixlen 64 scopeid 0x0<global>
              inet6 2409:4050:2d92:27eb:a00:27ff:fe13:932a prefixlen 64 scopeid 0x0<global>
                ether 08:00:27:13:93:2a txqueuelen 1000 (Ethernet)
                  RX packets 1203 bytes 94921 (92.6 KiB) RX bytes from given file
                  RX errors 0 dropped 0 overruns 0 frame 0
                  TX packets 8949 bytes 570375 (557.0 KiB) TX bytes to host
                  TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
      inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
          loop txqueuelen 1000 (Local Loopback)
            RX packets 20 bytes 996 (996.0 B) RX bytes to main name (which is
            RX errors 0 dropped 0 overruns 0 frame 0 main name (which is
            TX packets 20 bytes 996 (996.0 B) TX bytes to host
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
root@kali:~#
```

On Windows, you used the ipconfig command. However, this command has a counterpart, ifconfig, which works on Linux. The ifconfig command is the short name for Interface Configuration.

Unlike the ipconfig command, the ifconfig command does not accept the /all parameter. Instead, you need to use the –a parameter to display the complete network adapter configuration.

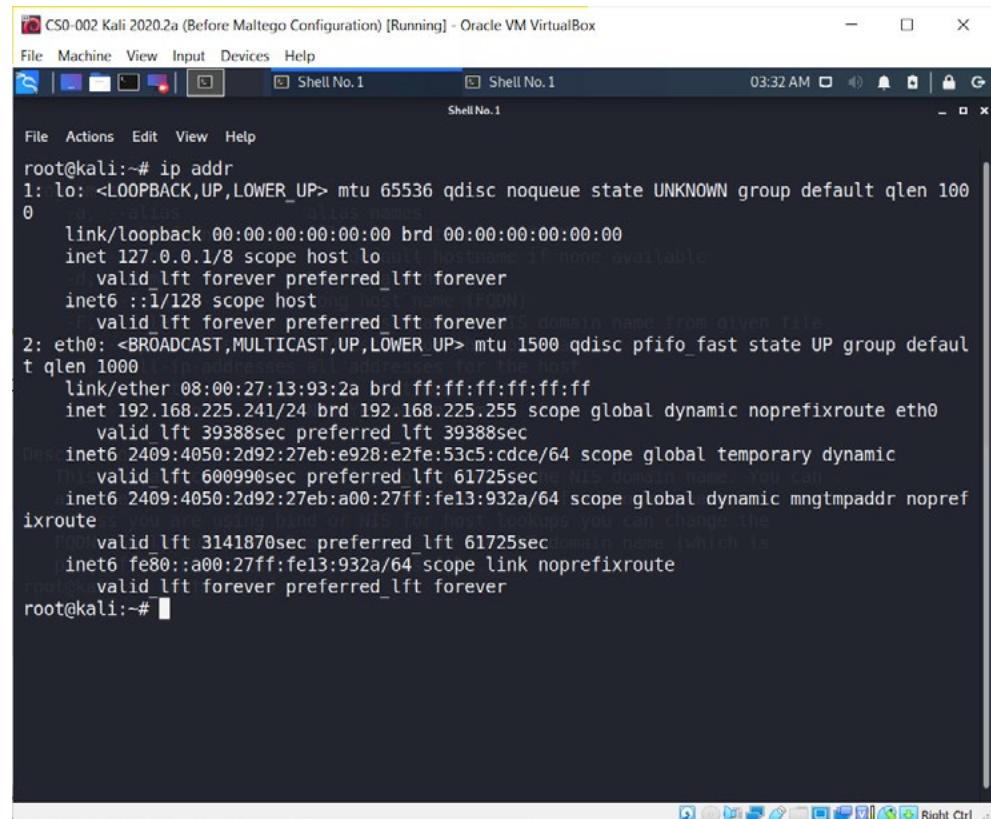
By default, the ifconfig command displays the complete information for all the available active network adapters, including the loopback adapter labeled as lo. However, you can choose to display the information for only a specific network adapter using the following command:

Ifconfig eth0

In this command, the network adapter name is eth0. When you execute this command, it does not show the configuration details of the lo or any other active network adapter. The ifconfig command works on all Linux and UNIX systems.

# ip

- Displays the IP addresses assigned to all or specific network interfaces in a system
- Can be used to assign or remove an IP address to a network interface
- Can change the network interface state to either UP or DOWN
- Works on Linux
- Example:
- ip a
- ip -4 a
- ip a add 192.168.1.1/255.255.255.0 dev eth0
- ip link set dev eth0 down



The screenshot shows a terminal window titled "CS0-002 Kali 2020.2a (Before Maltego Configuration) [Running] - Oracle VM VirtualBox". The window contains the output of the "ip addr" command run as root. The output details the configuration of network interfaces lo and eth0. Interface lo has an IPv4 address 127.0.0.1/8. Interface eth0 has an IPv4 address 192.168.225.241/24 and an IPv6 address fe80::a00:27ff:fe13:932a/64.

```
root@kali:~# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
            inet6 ::1/128 scope host
                valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:13:93:2a brd ff:ff:ff:ff:ff:ff
        inet 192.168.225.241/24 brd 192.168.225.255 scope global dynamic noprefixroute eth0
            valid_lft 39388sec preferred_lft 39388sec
        inet6 2409:4050:2d92:27eb:e928:e2fe:53c5:cdce/64 scope global temporary dynamic
            valid_lft 600990sec preferred_lft 61725sec
        inet6 2409:4050:2d92:27eb:a00:27ff:fe13:932a/64 scope global dynamic mngtmpaddr noprefixroute
            valid_lft 3141870sec preferred_lft 61725sec
        inet6 fe80::a00:27ff:fe13:932a/64 scope link noprefixroute
            valid_lft forever preferred_lft forever
root@kali:~#
```

Nslookup is the short name for Name Server Lookup. It is used to query the nameserver to get the domain name or the IP address. For example, you can use the following command to find the address record for a domain:

```
nslookup google.com
```

By default, with this command, the nslookup command displays the A record for the specified domain. When you execute this command, it sends a query to the domain's name server to get this information. After the information is received, it is displayed as the output.

The nslookup can also perform reverse DNS lookups. To do this, instead of the domain name, you need to provide the IP address of the domain:

```
Nslookup 13.77.161.179
```

If you do not specify any record, it then searches for the A record. However, you can search for a specific type of record by specifying its type.

```
nslookup -type=ns facebook.com
```

If you want to get the information for all types of records at once, you need to use the following command:

```
nslookup -type=any facebook.com
```

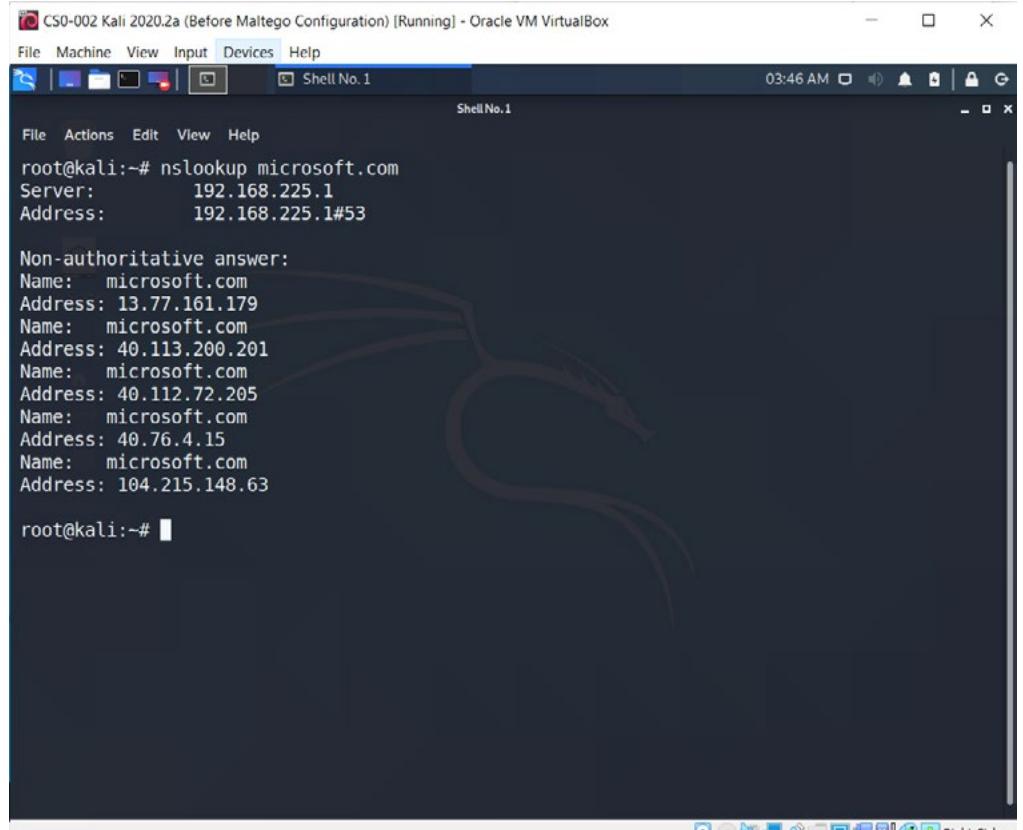
The type of records should be set to ANY.

Some of the key types of records are:

- MX = Mail Exchange. Provides the mail exchange servers for the domain
- SOA = Start of Authority. Provides the authoritative information for the domain, including the domain serial number, its origin, and mail address.
- NS = Name Servers. Provides the list of authoritative domain servers for the domain
- TXT = Text Records. Provides information about various other records, such as SPF and DKIM
- CNAME: Canonical Name. Provides the information about the alias for the domain name, which is the hostname to another hostname.
- AAAA: Quad A. Provides the information similar to the A record but in the IPv6 format.

# nslookup

- Stands for Name Server Lookup
- Queries a nameserver to get the domain name or the IP address
- Can perform reverse DNS lookups
- Can also find other types of records, such as MX, SOA, AAAA, CNAME, and TXT
- Works on Linux and Windows
- Example:
  - nslookup facebook.com
  - nslookup -type=ns facebook.com
  - nslookup -type=any facebook.com



The screenshot shows a terminal window titled "CS0-002 Kali 2020.2a (Before Maltego Configuration) [Running] - Oracle VM VirtualBox". The window has tabs for File, Machine, View, Input, Devices, and Help. The main area shows the command "nslookup microsoft.com" being run by a root user. The output includes an authoritative answer from a server at 192.168.225.1 and a non-authoritative answer from multiple other servers, including 13.77.161.179, 40.113.200.201, 40.112.72.205, 40.76.4.15, and 104.215.148.63.

```
root@kali:~# nslookup microsoft.com
Server:      192.168.225.1
Address:     192.168.225.1#53

Non-authoritative answer:
Name:  microsoft.com
Address: 13.77.161.179
Name:  microsoft.com
Address: 40.113.200.201
Name:  microsoft.com
Address: 40.112.72.205
Name:  microsoft.com
Address: 40.76.4.15
Name:  microsoft.com
Address: 104.215.148.63

root@kali:~#
```

# nslookup

Nslookup is the short name for Name Server Lookup. It is used to query the nameserver to get the domain name or the IP address. For example, you can use the following command to find the address record for a domain:

```
nslookup google.com
```

By default, with this command, the nslookup command displays the A record for the specified domain. When you execute this command, it sends a query to the domain's name server to get this information. After the information is received, it is displayed as the output.

The nslookup can also perform reverse DNS lookups. To do this, instead of the domain name, you need to provide the IP address of the domain:

```
Nslookup 13.77.161.179
```

If you do not specify any type of record, it then searches for the A record. However, you can search for a specific type of record by specifying its type.

```
nslookup -type=ns facebook.com
```

If you want to get the information for all types of records at once, you need to use the following command:

```
nslookup -type=any facebook.com
```

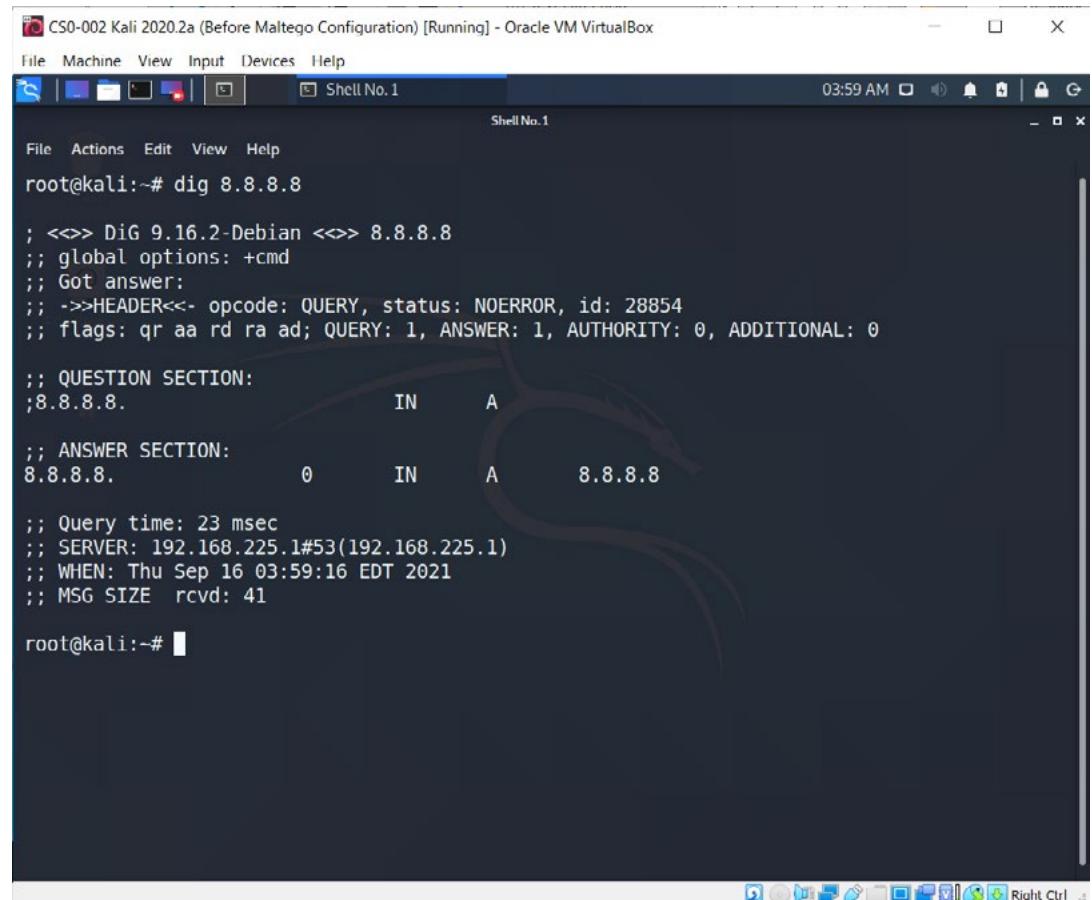
The type of records should be set to ANY.

Some of the key types of records are:

- MX = Mail Exchange. Provides the mail exchange servers for the domain
- SOA = Start of Authority. Provides the authoritative information for the domain, including the domain serial number, its origin, and mail address.
- NS = Name Servers. Provides the list of authoritative domain servers for the domain
- TXT = Text Records. Provides information about various other records, such as SPF and DKIM
- CNAME: Canonical Name. Provides the information about the alias for the domain name, which is the hostname to another hostname.
- AAAA: Quad A. Provides the information similar to the A record but in the IPv6 format.

# dig

- Stands for Domain Information Groper
- Is used for querying the DNS servers
- Is mainly used for DNS troubleshooting
- Can query host addresses
- Queries the /etc/resolv.conf file for the listed DNS servers
- Works on Linux and UNIX systems
- Examples:
  - dig -x 8.8.8.8
  - dig facebook.com
  - dig facebook.com MX



The screenshot shows a terminal window titled "Shell No.1" running on a Kali Linux system. The command entered is "dig 8.8.8.8". The output shows a standard DNS query response:

```
root@kali:~# dig 8.8.8.8

; <>> DiG 9.16.2-Debian <>> 8.8.8.8
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 28854
;; flags: qr aa rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;8.8.8.8.          IN      A

;; ANSWER SECTION:
8.8.8.8.          0       IN      A      8.8.8.8

;; Query time: 23 msec
;; SERVER: 192.168.225.1#53(192.168.225.1)
;; WHEN: Thu Sep 16 03:59:16 EDT 2021
;; MSG SIZE rcvd: 41

root@kali:~#
```

# dig

Dig stands for Domain Information Groper. One of the key commands is to query the DNS servers for various information, such as host addresses, mail exchange records, and name servers. The dig command takes the domain name as the parameter to display the information, the A record, NS record, and AAAA records if available.

To get this information, you need to use the following command:

```
dig facebook.com
```

When you execute the command, it provides the information in various sections. The output in the first section displays the version of the dig command. The second section displays the answer that was received for the query that you sent. The question section displays the domain name or the IP address passed as an argument to the dig command. In this case, it was facebook.com. Then, the answer section displays the answer received in response to the query. The Authority section, which may not be displayed in all queries if there are no authoritative name servers, displays the nameservers that have the authority to respond to the query. The Additional section displays more information about the authoritative servers that were listed in the Authority section.

You can also query the host addresses to find out more information about the domains. For example, let's say that you need to perform the reverse lookup using an IP address. To do this, you need to execute the following command:

```
dig -x 8.8.8.8
```

The -x parameter helps you perform the reverse lookup. If you do not use the -x parameter, only the IP address you queried is returned.

When you execute a dig command, it refers to the DNS servers listed in the /etc/resolv.conf file. Using the dig command, you can also query different types of records for the specified Website. For example, you can only query the MX records:

```
dig facebook.com MX
```

This query will return the mail exchange servers for the domain.



# traceroute

- Displays the route or path to a remote system
- Displays the number of hops to the destination
- Sends three ICMP packets
- Can display maximum of 30 hops
- Works on Linux and UNIX
- Examples:
  - traceroute google.com
  - Traceroute -h 20 google.com

```
jiofi.local.html (192.168.225.1) 5.936 ms 5.885 ms 5.864 ms
* * *
56.8.176.141 (56.8.176.141) 41.402 ms 56.8.176.93 (56.8.176.93) 41.388 ms 56.8.176.1
13 (56.8.176.113) 41.374 ms
192.168.44.234 (192.168.44.234) 41.360 ms 192.168.44.238 (192.168.44.238) 41.345 ms
192.168.44.234 (192.168.44.234) 57.966 ms
192.168.44.34 (192.168.44.34) 57.946 ms 192.168.44.239 (192.168.44.239) 57.932 ms 19
2.168.44.235 (192.168.44.235) 57.918 ms
172.26.100.118 (172.26.100.118) 57.904 ms 48.936 ms 48.895 ms
172.26.100.102 (172.26.100.102) 50.046 ms 172.26.100.103 (172.26.100.103) 24.366 ms
24.324 ms
192.168.44.22 (192.168.44.22) 39.701 ms 192.168.44.24 (192.168.44.24) 39.685 ms 192.
168.44.28 (192.168.44.28) 39.669 ms
192.168.44.23 (192.168.44.23) 40.022 ms 192.168.44.25 (192.168.44.25) 39.995 ms 192.
168.44.23 (192.168.44.23) 39.986 ms
172.16.26.5 (172.16.26.5) 39.943 ms 172.16.18.33 (172.16.18.33) 44.494 ms 40.334 ms
172.16.26.2 (172.16.26.2) 39.909 ms 172.16.26.0 (172.16.26.0) 46.483 ms 172.16.26.2
(172.16.26.2) 39.918 ms
142.250.168.56 (142.250.168.56) 39.890 ms 43.354 ms 74.125.147.192 (74.125.147.192)
40.029 ms
* * *
142.251.52.214 (142.251.52.214) 41.770 ms 142.251.76.172 (142.251.76.172) 41.731 ms
142.251.54.86 (142.251.54.86) 63.444 ms
142.251.54.83 (142.251.54.83) 62.576 ms 108.170.251.119 (108.170.251.119) 59.089 ms
108.170.251.107 (108.170.251.107) 56.017 ms
dell1s16-in-f14.1e100.net (142.250.193.78) 55.382 ms 74.125.244.193 (74.125.244.193)
55.959 ms dell1s16-in-f14.1e100.net (142.250.193.78) 39.845 ms
root@kali:~#
```

The traceroute command helps you determine the route or path to a remote system. It also helps you determine the total number of hops, or the intermediary routers, that come on the way. For example, let's assume that you execute the following command:

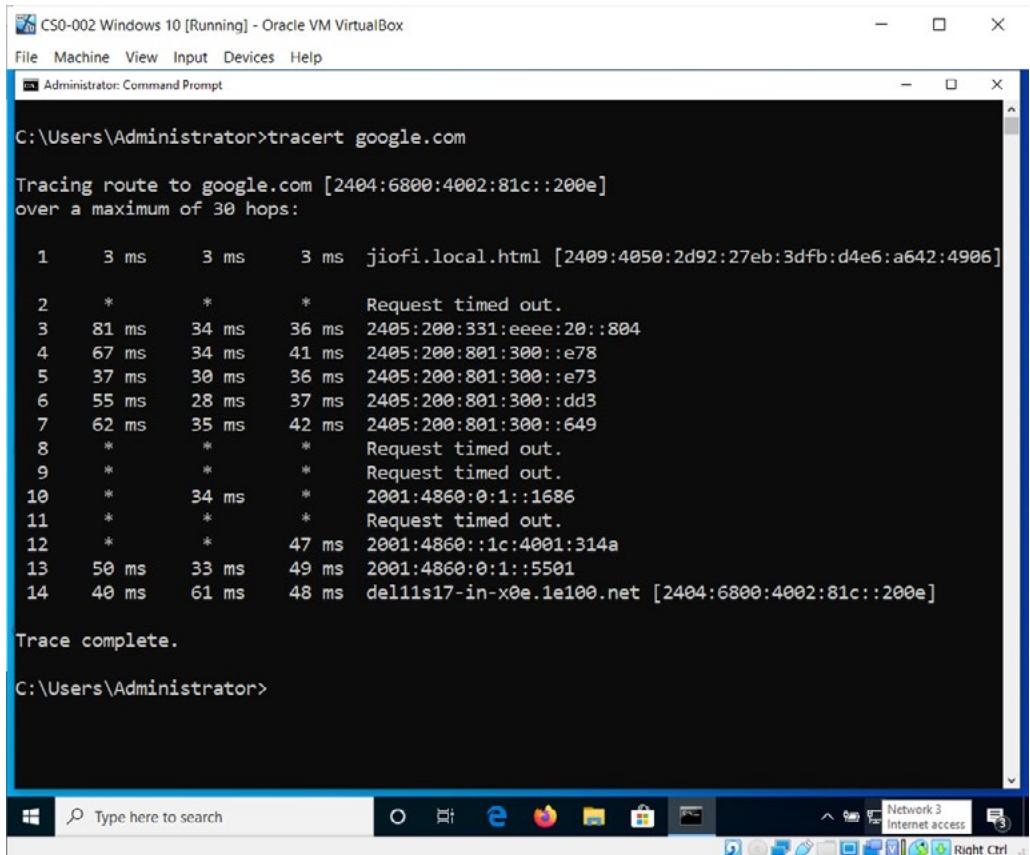
traceroute 8.8.8

From the starting point to the destination, there are several locations that the traceroute command will cross. Each location is called a hop. The tracert command sends three ICMP packets to each hop. The time taken by each packet to reach that particular hop is mentioned in the output of the traceroute command. The traceroute command has the limitation of 30 hops, which means that it cannot go beyond this limit. This command works only on Linux and UNIX. However, it has a similar command named tracert, which you will look at next.



# tracert

- Works in the same way as the traceroute command
- Works only on Windows
- Example:
  - tracert google.com
  - tracert 8.8.8.8
  - tracert -h 20 8.8.8.8



The screenshot shows a Windows 10 desktop with an Oracle VM VirtualBox window titled "CS0-002 Windows 10 [Running]". Inside the virtual machine, a Command Prompt window is open with the administrator privileges. The user has run the command "tracert google.com". The output shows the tracing route to google.com over 14 hops. Hops 1 through 13 show varying latency times (e.g., 3 ms, 81 ms, 67 ms, etc.). Hops 10, 11, and 12 are marked with an asterisk (\*) and labeled "Request timed out.". Hop 14 shows the final destination: "dell11s17-in-x0e.1e100.net [2404:6800:4002:81c::200e]". The command prompt ends with "Trace complete." and a prompt for the next command.

```
C:\Users\Administrator>tracert google.com

Tracing route to google.com [2404:6800:4002:81c::200e]
over a maximum of 30 hops:

 1    3 ms    3 ms    3 ms  jiofi.local.html [2409:4050:2d92:27eb:3dfb:d4e6:a642:4906]
 2    *        *        *        Request timed out.
 3    81 ms   34 ms   36 ms  2405:200:331:eeee:20::804
 4    67 ms   34 ms   41 ms  2405:200:801:300::e78
 5    37 ms   30 ms   36 ms  2405:200:801:300::e73
 6    55 ms   28 ms   37 ms  2405:200:801:300::dd3
 7    62 ms   35 ms   42 ms  2405:200:801:300::649
 8    *        *        *        Request timed out.
 9    *        *        *        Request timed out.
10    *        34 ms   *        2001:4860:0:1::1686
11    *        *        *        Request timed out.
12    *        *        47 ms  2001:4860:1c:4001:314a
13    50 ms   33 ms   49 ms  2001:4860:0:1::5501
14    40 ms   61 ms   48 ms  dell11s17-in-x0e.1e100.net [2404:6800:4002:81c::200e]

Trace complete.

C:\Users\Administrator>
```

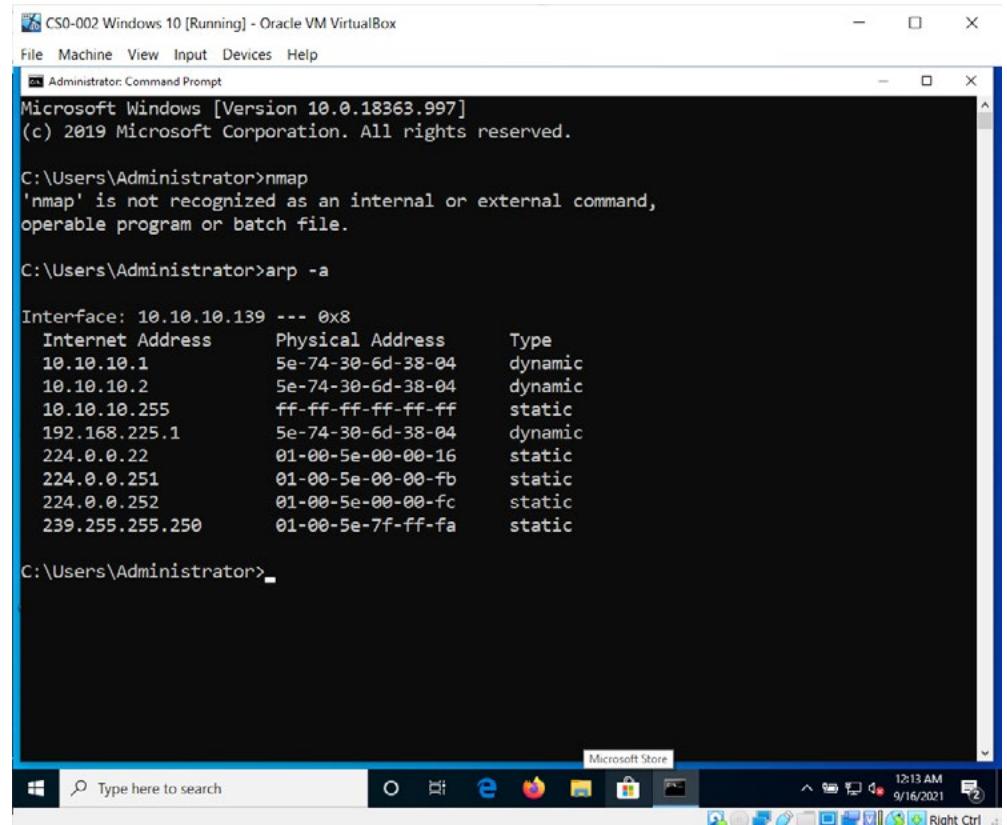
The tracert command works only on Windows and is similar to the traceroute command on Linux and UNIX. You can execute it to use either IPv4 or IPv6 in the following manner:

```
tracert -6 google.com
tracert -4 google.com
```

Most of the options in tracert work as the traceroute command. However, you can look at its help to determine more parameters.

# arp

- Displays the arp cache on a host
- Resolves the IP address to MAC address
- Allows you to manipulate the cache
- Works on Linux and Windows
- Example:
  - arp -a
  - arp -s 192.168.1.2 00-aa-00-62-c6-09



The screenshot shows a Microsoft Windows 10 Command Prompt window titled "CS0-002 Windows 10 [Running] - Oracle VM VirtualBox". The window displays the following text:

```
Microsoft Windows [Version 10.0.18363.997]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>nmap
'nmap' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Administrator>arp -a

Interface: 10.10.10.139 --- 0x8
  Internet Address      Physical Address      Type
  10.10.10.1            5e-74-30-6d-38-04  dynamic
  10.10.10.2            5e-74-30-6d-38-04  dynamic
  10.10.10.255          ff-ff-ff-ff-ff-ff  static
  192.168.225.1          5e-74-30-6d-38-04  dynamic
  224.0.0.22             01-00-5e-00-00-16  static
  224.0.0.251            01-00-5e-00-00-fb  static
  224.0.0.252            01-00-5e-00-00-fc  static
  239.255.255.250        01-00-5e-7f-ff-fa  static

C:\Users\Administrator>
```

The taskbar at the bottom of the screen shows various icons for Microsoft Store, File Explorer, Edge, and other system utilities. The system tray indicates the date as 9/16/2021 and the time as 12:13 AM.

# arp

Arp stands for Address Resolution Protocol that defines the mapping of an IP address to a MAC or the physical address of a network interface. You can use it to display the arp cache on a host. On Windows, you need to run the following command:

```
arp -a
```

On Linux, you can run the arp command to view the arp cache.

When a system needs to find the MAC address for an IP address, it adds the mapping to the ARP cache. This entry is used when next time the system needs to refer to the same MAC address. The arp command behaves slightly differently on Windows and Linux. If you execute it on Windows without any parameter, it lists the help information. However, on Linux, it displays the arp cache.

You can display all arp cache entries with the following command:

```
arp -a
```

You can also manipulate the arp cache. For example, you can delete an arp cache entry for a specific host with the following command:

```
arp -d localsystem
```

The -d parameter is the parameter, and the hostname, the localsystem, is the argument you need to pass to the arp command.

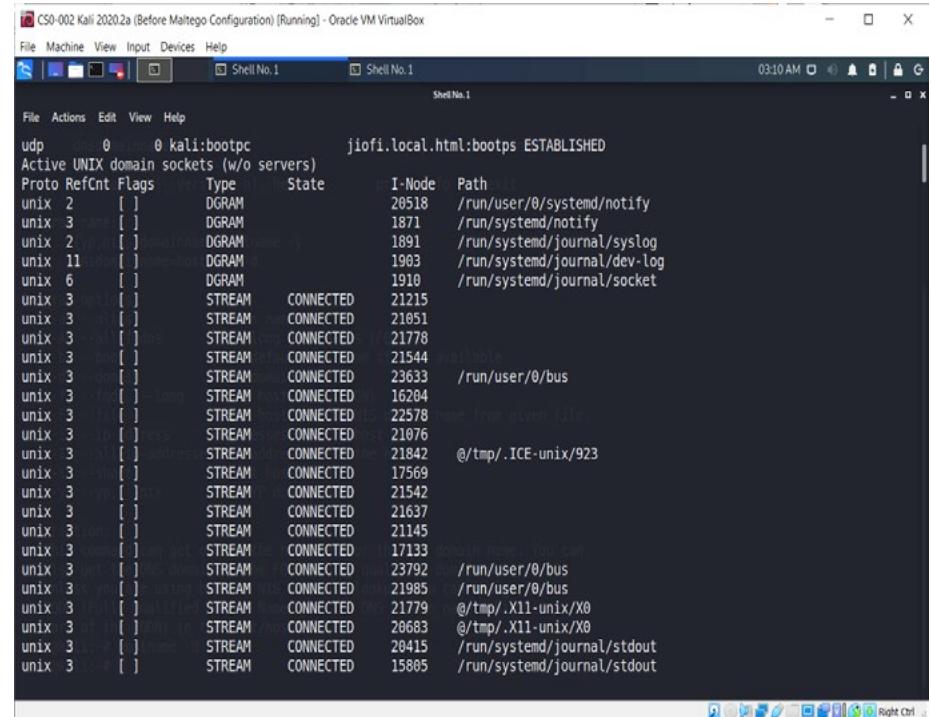
Using the -s parameter, you can also add a static arp entry:

```
arp -s 192.168.1.2 00-aa-00-62-c6-09
```



# netstat

- Is short name for Network Statistics
- Displays the following information:
  - Routing-table entries
  - Active connections
  - Ports
  - Protocols
- Active network interface statistics
- Works on Linux and Windows
- Example:
  - netstat
  - netstat -a
  - netstat -f



```
CS0-002 Kali 2020.2a (Before Maltego Configuration) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Shell No.1 Shell No.1 Shell No.1
File Actions Edit View Help
Proto RefCnt Flags Type State I-Node Path
udp 0 kali:bootpc jiofil.local.html:bootps ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags Type State I-Node Path
unix 2 [ ] DGRAM
unix 3 [ ] DGRAM
unix 2 [ ] DGRAM
unix 11 [ ] DGRAM
unix 6 [ ] DGRAM
unix 3 [ ] STREAM CONNECTED 21215
unix 3 [ ] STREAM CONNECTED 21051
unix 3 [ ] STREAM CONNECTED 21778
unix 3 [ ] STREAM CONNECTED 21544
unix 3 [ ] STREAM CONNECTED 23633 /run/user/0/bus
unix 3 [ ] STREAM CONNECTED 16284
unix 3 [ ] STREAM CONNECTED 22578
unix 3 [ ] STREAM CONNECTED 21076
unix 3 [ ] STREAM CONNECTED 21842 @/tmp/.ICE-unix/923
unix 3 [ ] STREAM CONNECTED 17569
unix 3 [ ] STREAM CONNECTED 21542
unix 3 [ ] STREAM CONNECTED 21637
unix 3 [ ] STREAM CONNECTED 21145
unix 3 [ ] STREAM CONNECTED 17133
unix 3 [ ] STREAM CONNECTED 23792 /run/user/0/bus
unix 3 [ ] STREAM CONNECTED 21985 /run/user/0/bus
unix 3 [ ] STREAM CONNECTED 21779 @/tmp/.X11-unix/X0
unix 3 [ ] STREAM CONNECTED 20683 @/tmp/.X11-unix/X0
unix 3 [ ] STREAM CONNECTED 20415 /run/systemd/journal/stdout
unix 3 [ ] STREAM CONNECTED 15805 /run/systemd/journal/stdout
```

Netstat is a short name for network statistics, both on Windows and Linux. When you execute this command, it can display the following output:

- Routing-table entries
- Active connections
- Ports
- Protocols
- Active network interface statistics

For example, you can use the -a parameter to display all active ports:

```
netstat -a
```

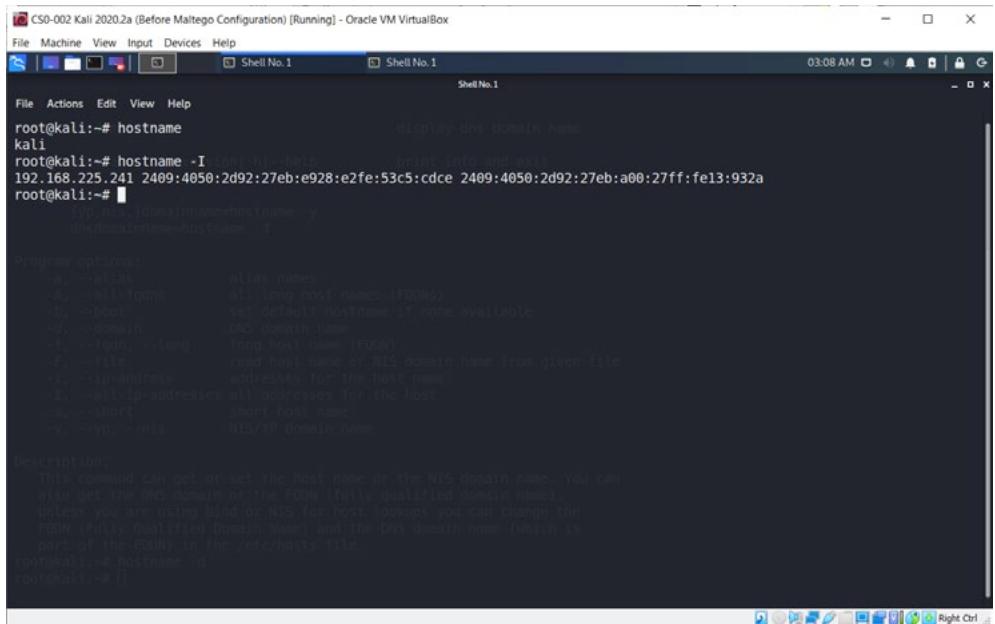
You can also view the network statistics on a specific interface using the -i parameter:

```
netstat -i
```



# hostname

- Is used to display the hostname
- Can also be used to set the hostname on Linux
- Can also display the IP addresses assigned to the host on Linux
- Can also be used to set the short name or long name for the host on Linux
- Example:
  - `hostname`
  - `hostname -a`



The screenshot shows a terminal window titled "CS0-002 Kali 2020.2a (Before Metasploit Configuration) [Running] - Oracle VM VirtualBox". The window has two tabs: "Shell No.1" and "Shell No.2". The current tab is "Shell No.1". The terminal prompt is "root@kali:~#". The user runs the command `hostname`, which outputs the current host name, "kali". Then, the user runs `hostname -I`, which outputs the IP address associated with the interface, "192.168.225.241". Below these commands, there is a "Program options:" section listing various parameters for the `hostname` command, such as `-a` for alias names, `-A` for all long host names (FQDN), `-d` for setting default hostname if none available, `-D` for DNS domain name, `-f` for reading host name or FQDN from given file, `-I` for addresses for the host name, `-L` for all IP addresses for the host, `-s` for short host name, and `-V` for version. At the bottom, there is a "description:" section explaining how the command can get or set the host name or the DNS domain name, mentioning the use of `idn` or `NIS` for host lookups and the `FQDN` (Fully Qualified Domain Name) and the `DNS` domain name (which is part of the `FQDN`) in the `/etc/hosts` file.

The `hostname` command displays the hostname on Windows and Linux. On Windows, it can only provide the hostname. However, Linux can use various parameters to display a variety of details.

It can also be used to display the IP addresses that are assigned to the network interfaces. To do this, you need to use the `-i` parameter:

`hostname -i`

The output can display the IPv4 and the IPv6 IP addresses, if any, is assigned to an interface. You can also use the `hostname` to list the short or long names. The short name is displayed with the `-s` parameter:

`hostname -s`

It returns only the hostname, such as the local system. However, the `-A` parameter displays the long name or the FQDN, the Fully Qualified Domain Name.

`hostname -A`

It returns the hostname as an FQDN, such as `localsystem.example.com`.

# route

- Displays the routing table data on a host
- Displays the routes to the hosts and networks
- Allows you to add or remove routes manually
- Refers to the /etc/hosts or the DNS (name server) for name resolution
- Works on Linux and Windows
- Example: route PRINT

```
C:\Users\Administrator>route PRINT
=====
Interface List
  8...08 00 27 9f d4 1e .....Intel(R) PRO/1000 MT Desktop Adapter
  1.....Software Loopback Interface 1
=====

IPv4 Route Table
=====
Active Routes:
Network Destination      Netmask        Gateway       Interface Metric
          0.0.0.0      0.0.0.0    10.10.10.1   10.10.10.139  281
          10.10.10.0  255.255.255.0  On-link        10.10.10.139  281
          10.10.10.139 255.255.255.255  On-link        10.10.10.139  281
          10.10.10.255 255.255.255.255  On-link        10.10.10.139  281
          127.0.0.0     255.0.0.0    On-link        127.0.0.1    331
          127.0.0.1     255.255.255.255  On-link        127.0.0.1    331
          127.255.255.255 255.255.255.255  On-link        127.0.0.1    331
          224.0.0.0     240.0.0.0    On-link        127.0.0.1    331
          224.0.0.0     240.0.0.0    On-link       10.10.10.139  281
          255.255.255.255 255.255.255.255  On-link        127.0.0.1    331
          255.255.255.255 255.255.255.255  On-link       10.10.10.139  281
=====
Persistent Routes:
 Network Address      Netmask  Gateway Address Metric
          0.0.0.0      0.0.0.0    10.10.10.1 Default
=====
```

There may be a need to know the routes that are added to your system. For example, you may want to view the routes to troubleshoot a connectivity issue on one of the hosts on a network. Whether running Windows or Linux, each system contains a routing table, which has the routes added when you are on the network, and the persistent routes, which are always there whether or not your system is connected to a network. The route command displays the routes to both IPv4 and IPv6 networks.

On Windows, you can display the routes using the following command:

```
route PRINT
```

It then displays the routes to the hosts and networks. You can also add or remove routes in a system. To add a route, you need to execute the following command:  
route add 10.10.10.0 MASK 255.0.0.0 10.10.0.1

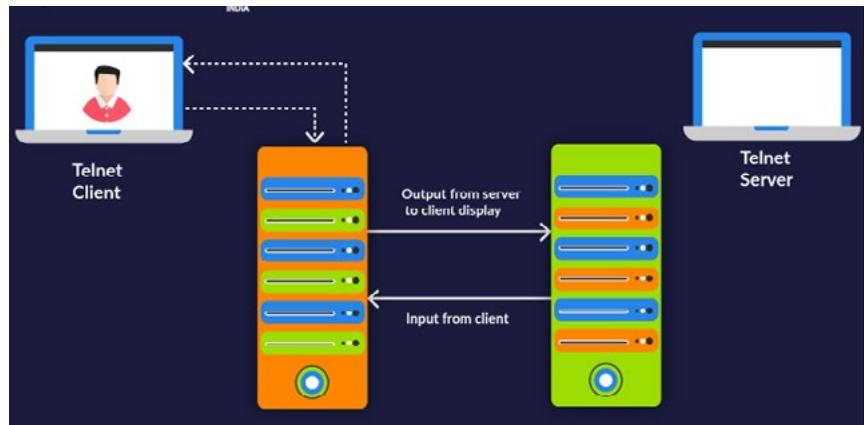
To delete a route:

```
route delete 10.10.10.0
```

The route command can refer to the etc/hosts or the DNS (name server) when performing the name resolution. You can use the route command on either Windows or Linux.

# telnet

- Is used for terminal access to a remote host
- Requires client software, such as Putty
- Uses TCP port 23
- Sends and receives information in unencrypted manner
- Is rarely used in current times
- Was used on Windows and Linux
- Example: telnet 192.168.1.2



<https://www.servercake.blog/what-is-telnet/>

Telnet is an obsolete protocol that was used to connect to a system remotely. It used to provide terminal access to a remote host, which needed to run a Telnet server. From the client, using a tool like Putty, you would need to connect to the server on TCP port 23. This meant that if the remote client was behind a firewall, the TCP port 23 needed to be opened. You could use Telnet to remotely connect and perform certain tasks like managing files and folders on the remote system.

Telnet is rarely used nowadays because of security reasons. It sends the information in clear text format, which means anyone can intercept the communication and read it. For example, when you enter the username and password over a Telnet session, anyone could intercept the traffic and get to know the username and password.

The Telnet command is simple:

telnet 192.168.1.2

The IP address is the remote system. You can either specify the IP address or the hostname if DNS is in place to perform name resolution. Alternatively, you can map the IP address with the hostname in your system's hosts file.

# tcpdump

- Helps to capture the TCP/IP packets in real-time
  - Is used for network analysis and troubleshooting
  - Allows you to save the packet capture in a pcap file
  - Works only on Linux and UNIX systems
  - Example:
    - `tcpdump`
    - `tcpdump -i eth0`

The `tcpdump` command is used to capture the TCP/IP packets in real-time to analyze them. It can capture, filter, and analyze the traffic that is being transmitted over a network. You can either view the information in real-time or save it for later use in the pcap file, which can then be used with the `-r` parameter, which allows you to read it from the pcap file. You can use the `-w` parameter to write the network traffic into the pcap file:

To write to a pcap file:

```
tcpdump -w test.pcap
```

To write to a pcap file, you need administrative privileges. If you are logged onto the Linux system as a regular user, you need to prefix the command with sudo, which provides administrative capabilities to execute the command.

To read from a ncan file:

to read from a pcap file

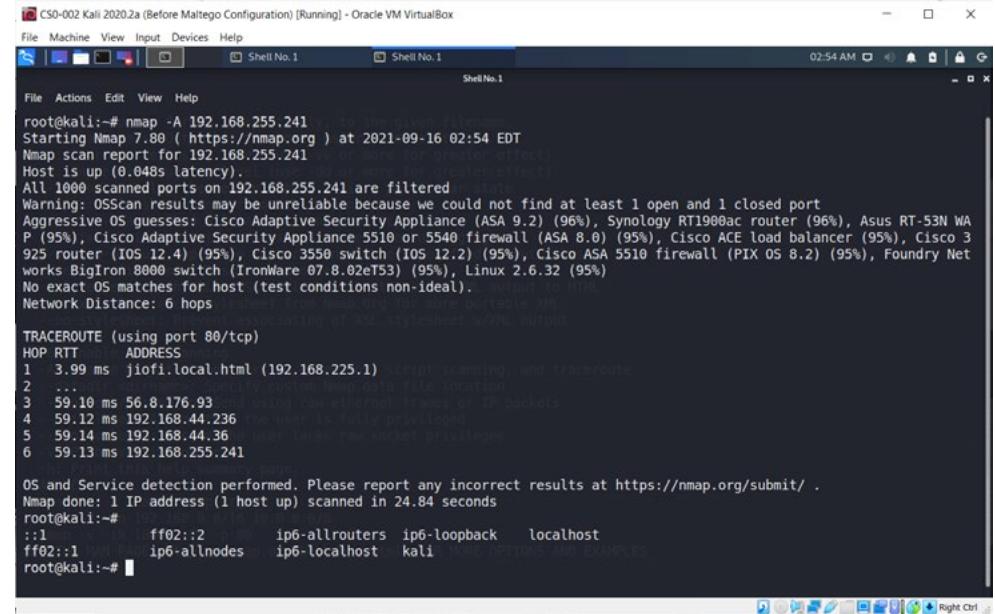
To use a specific interface with tcndump:

to use a specific interface:

The `tcpdump` command works only on Linux and UNIX.

# nmap

- Is short name for Network Mapper
- Can be used to check running services and open ports on a host
- Can be used to check live hosts on the network
- Can be used to determine the operating system of the remote host
- Can collect information to determine a logical network map
- Example:
- nmap 192.168.0.1
- nmap -A 192.168.0.1



The screenshot shows a terminal window titled "CS0-002 Kali 2020.2a (Before Metasploit Configuration) [Running] - Oracle VM VirtualBox". The terminal displays the results of an nmap scan. The command run was "nmap -A 192.168.255.241". The output includes:  
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-16 02:54 EDT  
Nmap scan report for 192.168.255.241  
Host is up (0.048s latency).  
All 1000 scanned ports on 192.168.255.241 are filtered  
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port  
Aggressive OS guesses: Cisco Adaptive Security Appliance (ASA 9.2) (96%), Synology RT1900ac router (96%), Asus RT-53N WA P (95%), Cisco Adaptive Security Appliance 5510 or 5540 firewall (ASA 8.0) (95%), Cisco ACE load balancer (95%), Cisco 3 925 router (IOS 12.4) (95%), Cisco 3550 switch (IOS 12.2) (95%), Cisco ASA 5510 firewall (PIX OS 8.2) (95%), Foundry Net works BigIron 8000 switch (IronWare 07.8.02eF53) (95%), Linux 2.6.32 (95%)  
No exact OS matches for host (test conditions non-ideal).  
Network Distance: 6 hops  
  
TRACEROUTE (using port 80/tcp)  
HOP RTT ADDRESS  
1 3.99 ms jiofilocal.html (192.168.225.1)  
2 ...  
3 59.10 ms 56.8.176.93  
4 59.12 ms 192.168.44.236  
5 59.14 ms 192.168.44.36  
6 59.13 ms 192.168.255.241  
  
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/.  
Nmap done: 1 IP address (1 host up) scanned in 24.84 seconds

# nmap

Nmap is a short name for the Network Mapper tool. It is one of the most widely used tools for network scanning and probing. With the nmap tool, you can perform various tasks, such as:

- Check for running servers
- Check for open ports
- Check for live hosts on the network
- Determine the operating system of a host
- Collect information to determine a logical network map

The nmap tool can be simply used with the hostname or the IP address to get its status for:

- Open ports
- Name of the host
- Number of closed ports

The command that you can use to get this information is:

```
nmap 192.168.1.2
```

The IP address is provided as the argument to the nmap command. You can also use various parameters to get more detailed information. For example, if you need to get the operating system details, you can use the -A parameter in the following manner:

```
nmap -A 192.168.1.2
```

The output provides detailed information about the open ports, running services, their versions, operating system name, and the number of hops in which the system is located.

Nmap has a large number of parameters that can be used. You can list these parameters using the --help parameter with the nmap command:

```
nmap --help
```

An alternate parameter to get the help is -h.





## *TOPIC 3*

---

# BASIC NETWORK PLATFORM COMMANDS

---

# Network Platform Commands

- Show Interface:
  - Shows interface status, IP address, input and output queues, and MAC address
- Show config:
  - Displays the current system configuration
- Show route:
  - Displays the routing table on a device

```
HQ_Router#show interface fa0/0
FastEthernet0/0 is up, line protocol is up (connected)
  Hardware is Lance, address is 0002.16c4.5301 (bia 0002.16c4.5301)
  Internet address is 10.0.0.5/8
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00,
  Last input 00:00:08, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0 (size/max/drops); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 input packets with dribble condition detected
    0 packets output, 0 bytes, 0 underruns
    0 output errors, 0 collisions, 1 interface resets
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier
    0 output buffer failures, 0 output buffers swapped out
```

The first command is the show interface command that displays the interface status, which includes:

- Current status of the interface
- The IP address of the interface
- Input and output queues on the interface
- MAC address of the interface

With the show config command, you can view the current configuration. With the show route command, it displays the routing table that exists on the device.

# Summary

- Software tools
- Command line tool
- Basic network platform commands



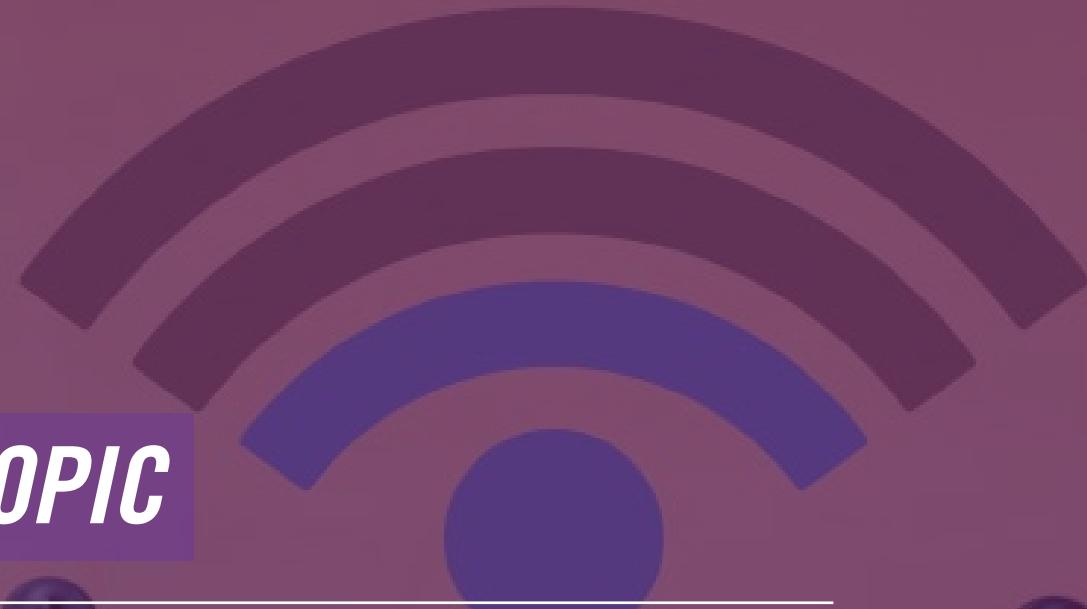
That's the end of the lesson.

Here we covered

- Software tools
- Command line tool
- Basic network platform commands



*NEXT TOPIC*



---

# WIRELESS CONNECTIVITY ISSUES

---

# 4

---

# Wireless Connectivity Issues

- 1 — Welcome to the 4 lesson of Module 5. In this lesson, you will learn about the:
  - 2 — Wireless Connectivity Issues
-

# Agenda

- Specifications and limitations
- Considerations
- Common issues



Hi, welcome to COMPTIA Network+ Course

In this lesson, we will talk about:

- Specifications and limitations
- Considerations
- Common issues





*TOPIC 1*

---

# SPECIFICATIONS AND LIMITATIONS

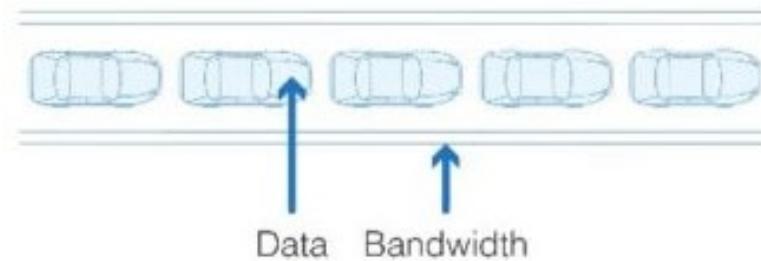
---

# Throughput

## Throughput:

One data packet arrives within one second.

- Is the amount of data transmitted from one system to another in a given time frame
- Is impacted due to:
  - Interference
  - Placement of electrical devices
- Can be increased by prioritizing the traffic



The wired and wireless networks need to have good throughput, which is the amount of data sent from one system or device to another in a specific time frame. In simplest terms, you can say that the amount of water running through a pipe is the throughput of the pipe. Similarly, the same concept applies to the wired or wireless network. It is the amount of data that can be sent or received in a given time frame.

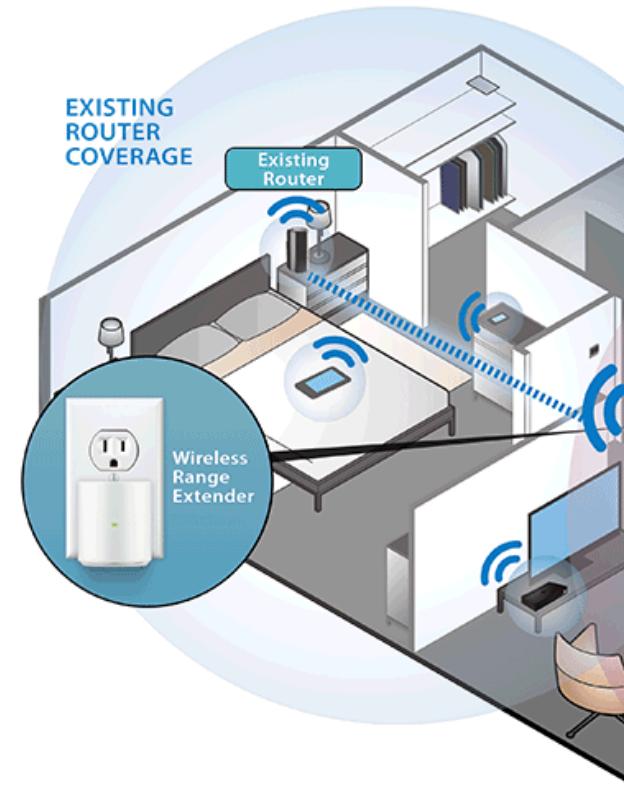
No network runs without issues. Throughput is one of the primary issues networks face – specifically in wireless networks. There can be various reasons or issues due to which the throughput of a wireless network can be impacted:

- Wireless networks work with specific frequencies, such as 2.4 or 5.0 GHz. Most of the electrical devices work with 2.4 GHz frequencies. You will learn about these later in the lesson. When the same frequency is used, it causes interference in the wireless network. You may have to place the electrical devices far away from the wireless router.
- Another major issue is the placement of antennas. Antennas are used for transmitting and receiving signals. Correct antenna placement provides good throughput. If the placement is incorrect, then the throughput is impacted.

The load on the wireless router can also be a reason for bad throughput. The solution to this is simple – prioritize the network traffic. For example, you may need to prioritize voice and video traffic over the data traffic.

# Distance

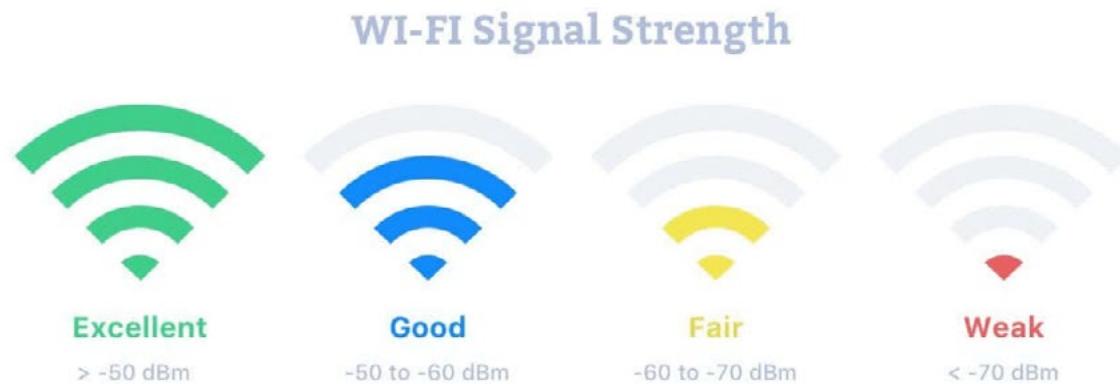
- Impacts the connectivity
  - Closer the client to the router, better the connectivity
  - Clients located far away may lose connectivity or get weaker signals
- Can be decreased by installing a wireless signal amplifier between the client and the wireless router



Distance between the wireless router and the user is another key factor. Several factors may contribute to it – walls, wooden doors, or simply the distance. The users should be closely located to the wireless router. If they are located far away, they are likely to get low connectivity or lose connectivity. There will always be areas in the office or home where signal strength is low. To solve such a problem, you need to install a wireless extender or repeater that extends the signals to areas they don't reach. It is important to note that the extender or the repeater extends or amplifies the signals, but they do not boost the speed or throughput.

# RSSI Signal Strength

- Is the signal strength received by an antenna on a wireless router
- Determines the quality of the signal
- Is calculated by:  
Total signal transmitted – signal loss = RSSI



The Received Signal Strength Indicator (RSSI) is the signal strength received by a wireless antenna on a wireless router. It determines wireless signal quality. You can calculate the signal quality by using the following formula:

The total signal transmitted – signal loss = RSSI

It is the value that determines the signal that a wireless client receives. It is important to note that the RSSI value will always be higher for the wireless devices placed near the wireless router. This is because the signal strength is much better and stronger, and therefore, the RSSI value is higher. The calculation is simple – the lesser the signal loss, the higher the RSSI value. For example, a value of -50 dBm is better than -70 dBm.

# EIRP Power Rating

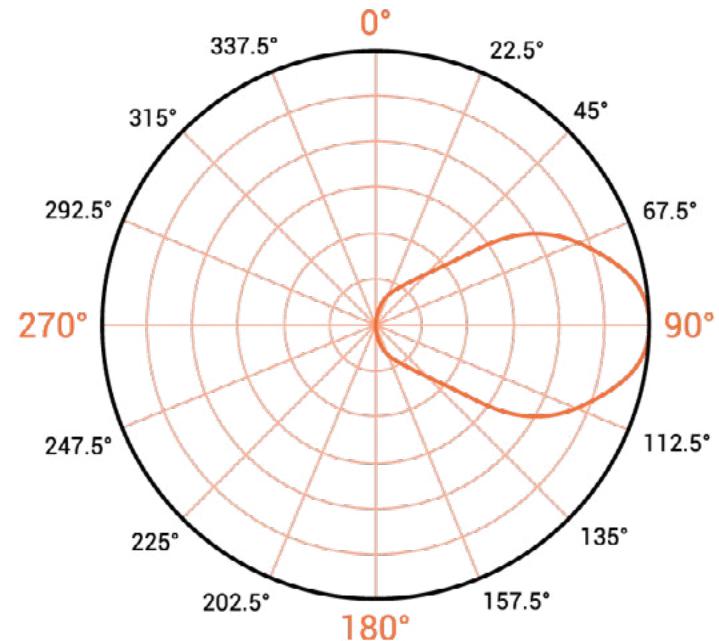
- Determines the antenna power in a direction
- Is defined in decibels over isotropic, dBi
- Is calculated by:
- $\text{EIRP} = \text{PT} - \text{LC} + \text{GTx}$

EIRP = effective isotropic radiated power in dB

PT = antenna's radiated power in dBW

LC = signal loss caused in dB

GTx = gain of the transmitting antenna in dB



[EIRP Calculator - Electrical Engineering & Electronics Tools \(allaboutcircuits.com\)](http://allaboutcircuits.com/electronics-tools/eirp-calculator/)

Effective Isotropic Radiated Power (EIRP) is the signal strength of an antenna. It is the maximum radiated power of an antenna in a specific direction. EIRP is calculated from the starting point of the transmission at the antenna.

The EIRP value is determined in decibels over isotropic, dBi.

EIRP is calculated by:

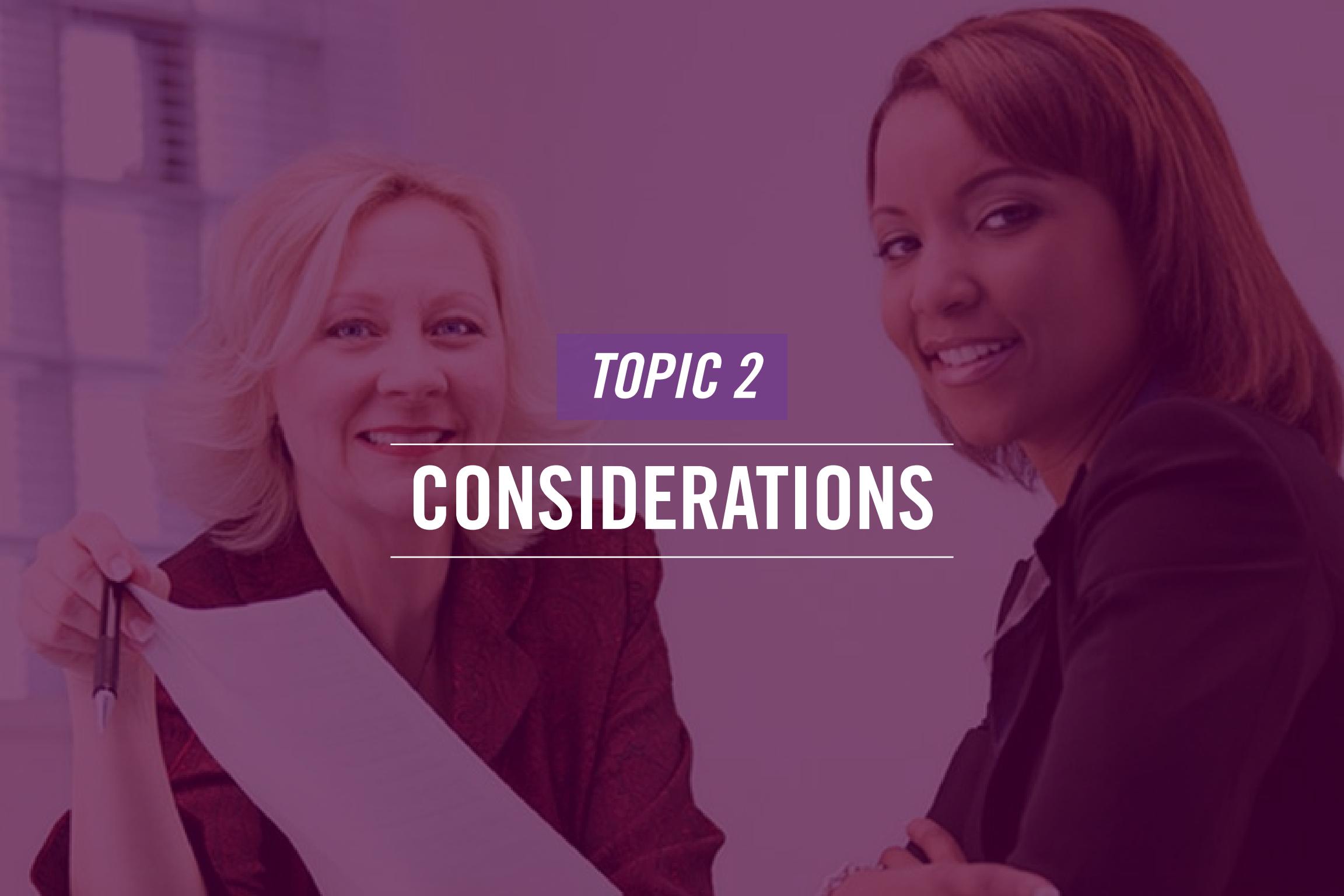
$$\text{EIRP} = \text{PT} - \text{LC} + \text{GTx}$$

EIRP = effective isotropic radiated power in dB

PT = antenna's radiated power in dBW

LC = signal loss caused in dB

GTx = gain of the transmitting antenna in dB

A photograph of two women in an office setting. On the left, a woman with blonde hair, wearing a red patterned blouse, holds a white paper and a pen, smiling at the camera. On the right, another woman with dark hair, wearing a dark blazer over a light shirt, also smiles. They appear to be in a professional environment, possibly reviewing documents together.

*TOPIC 2*

---

## CONSIDERATIONS

---

# Antennas

- Placement
  - Impacts the wireless network performance
  - Should have one antenna horizontally and one vertically aligned
- Types
  - Directional
  - Omnidirectional
- Polarization
  - Orientation of the antenna concerning the surface of the earth



As you have already learned, antennas play a critical role in a wireless network. There are three factors about antennas that you must know. The first factor is placement. You need to place the wireless router in such a position that there is a clear line of sight between the router and the wireless device. If there are obstacles, the wireless network performance will be impacted. The wireless router's antenna should be placed horizontally, and the second one should be placed vertically.

When you talk about antennas, there are essentially two types:

- Directional: They are meant to send signals in a specific direction. This type of antenna can extend the signals to a dead zone. An example of a directional antenna is a dish antenna.
- Omnidirectional: They broadcast the signals in all directions. They are mainly used with point-to-point connections. Most wireless routers will have omnidirectional antennas.

Antenna polarization is the antenna's orientation concerning the surface of the earth. It could be vertical or horizontal. Depending on the position of the electric field, whether vertical or horizontal, the antenna is polarized in the same way.

# Channel Utilization

- Are selected automatically when a wireless router is configured
- Can be overburdened if too many clients connect to the same channel
- Is achieved best when clients are using different channels
- Is best to configure dynamic allocation



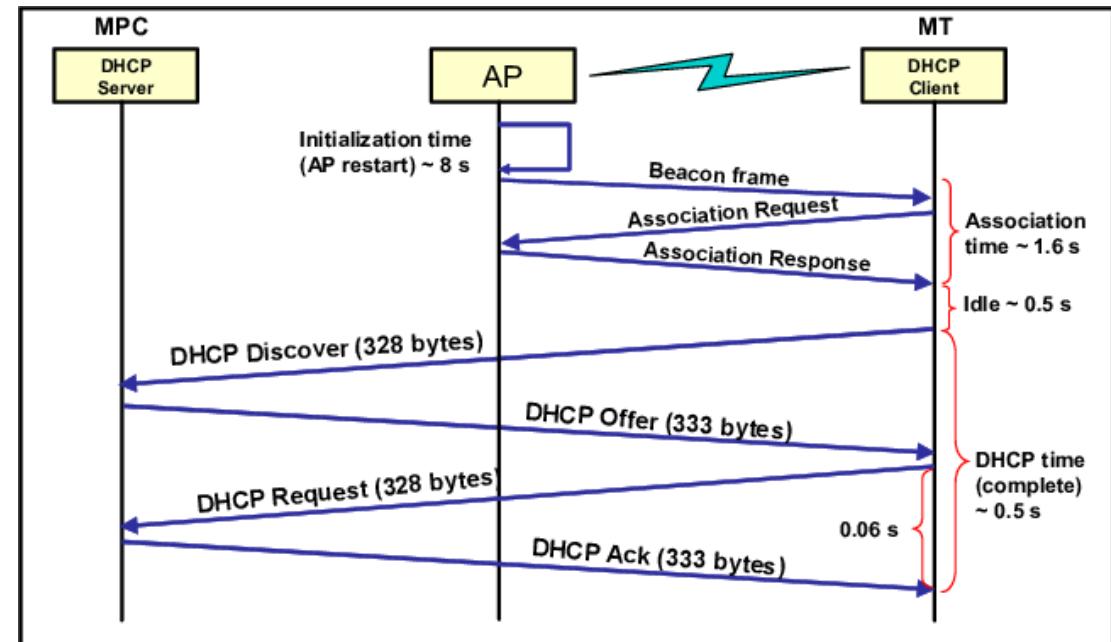
You usually do not configure the channel when you install a wireless router. The wireless router automatically configures it for you. When a wireless client, a mobile device, or a laptop connects to the wireless router, it detects the channel being used by the wireless router. The wireless client then automatically connects using the channel configured by the wireless router.

If all wireless clients start to connect using the same channel, then the channel may be overburdened. In this case, you should configure the wireless router to allow some of the clients to use a different channel than the one they were connecting with. For example, you may have your smart TV connecting on one channel but the rest of the device on another channel. Using this method, you can increase the wireless network performance by distributing the traffic over different channels.

Some wireless routers also allow you to configure dynamic channel allocation to wireless clients. It is a good feature because it helps you avoid channel overloading by allocating different channels.

# AP Association Time

- Is the time a client is associated or connected with a wireless router
- Is with only one wireless network at a time



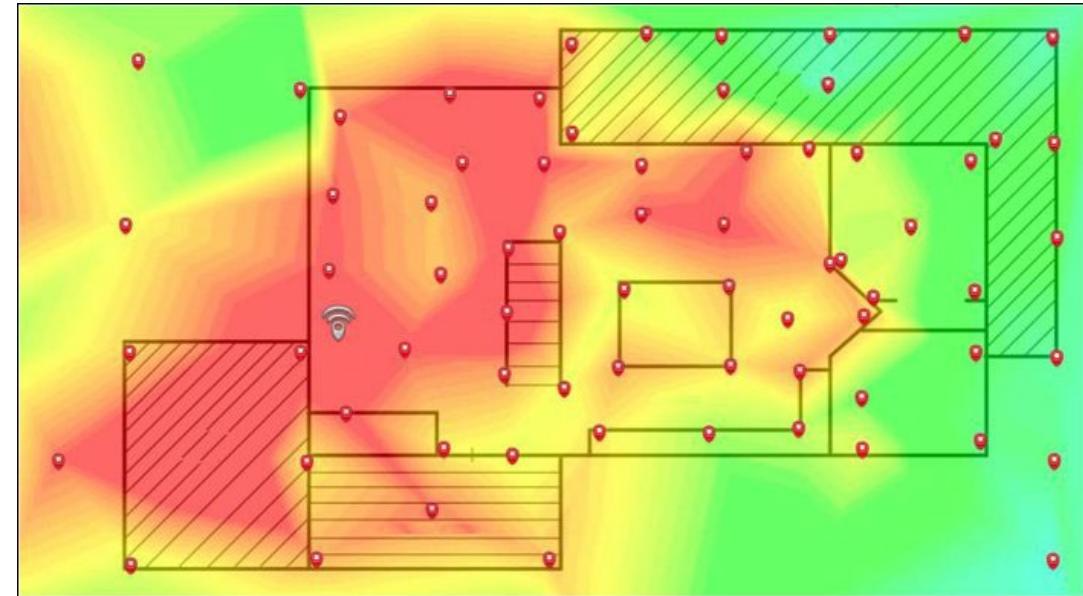
When a wireless client connects to the wireless router, it gets authenticated. After the authentication, the wireless client is registered on the wireless router. After the client is registered, it is associated with the wireless network. Each wireless client connects to the wireless network for a specific time. It could be a few minutes or a few hours. The time the wireless client is connected is known as the association time.

During this association, a dynamic IP can also be assigned using the DHCP server running on the wireless router. It is important to note that the client association process occurs when the wireless network is configured in the infrastructure mode.

A wireless client can only associate with one wireless network at a time. To associate with another wireless network, it must first dissociate itself from the current wireless network. However, a wireless client can associate with the mobile data and wireless network simultaneously. For example, you can activate the mobile data on your mobile device and still connect to a wireless network.

# Site Survey

- Are used to map the entire site
- Are used to identify interference and the blind spots
- Can help to determine the speed
- Help you determine the appropriate configuration



Before installing a wireless network, you should perform a site survey. It is required to map the entire physical site and figure out a few key issues that may disrupt the connectivity. Some of the key issues are blind spots and interferences.

With the help of the site survey, you can also determine the speed of the wireless network. You can figure out the number of wireless access points required for a physical site. You can even determine where the wireless access points will be installed. In some dead zones or areas where wireless access points cannot be installed, you may even use wireless extenders or repeaters.

In a nutshell, you can decide and determine the configuration for a wireless network using a site survey.



*TOPIC 3*

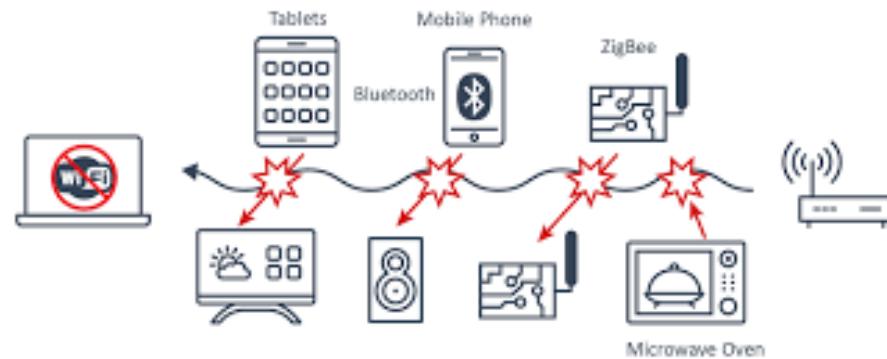
---

# COMMON ISSUES

---

# Interference

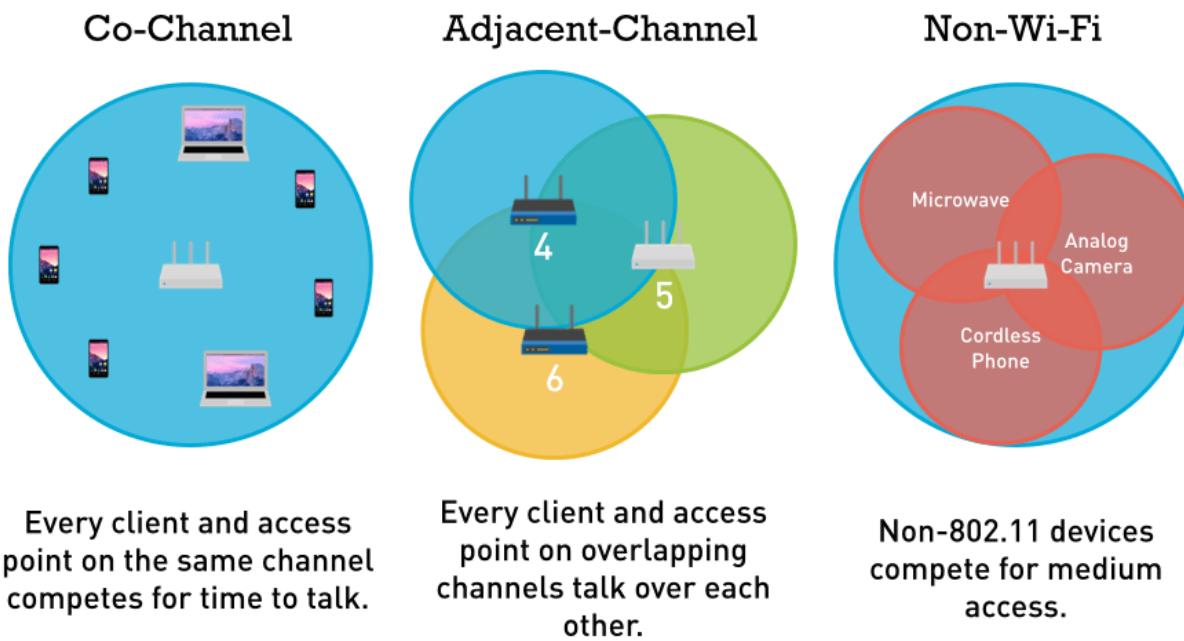
- Is generated by home appliances
  - They use 2.4 GHz frequency
  - Wireless networks mostly use 2.4 GHz frequency as well
- Is generated by:
  - Mobile phones
  - Microwaves
  - Bluetooth
- Results in:
  - Poor network performance
  - Latency and jitter



Several home appliances use the 2.4 GHz frequency – the same frequency as most wireless networks, such as 802.11b, g, n, and ax. Even though 802.11n and ax can also work on 5.0 GHz frequencies for faster speed, they are generally preferred with 2.4 GHz because it provides a long connectivity range. When both the home appliance and the wireless networks work with the 2.4 GHz frequency, an obvious interference is generated.

It is obvious to have mobile phones, microwaves, and Bluetooth devices, such as smartwatches and headphones, at home. However, the users are mostly unaware that these devices cause interference to the wireless network, causing performance deterioration. Along with the poor performance, there can also be latency and jitter getting introduced into the network.

# AP Association Time



The 2.4 GHz spectrum works with 11 channels that mostly overlap with each other. When there are overlapping channels, they attempt to communicate, causing the adjacent-channel interference. Then you have the co-channel interference caused by too many devices attempting to connect to the same channel. These devices virtually compete to get their share of time on these channels. Finally, some devices cause interference, which eventually increases the time for requests to be serviced. Most of these interferences take place with the channels that overlap each other. To improve the problem and detect interference, you can use tools like inSSIDer, which helps you detect the interference and the correct channel to choose.

You should use channels 1, 6, and 11 on the 2.4 GHz frequency to get the best wireless network performance. These are non-overlapping channels

# Antenna Cable Attenuation/Signal Loss

- Is the attenuation that occurs due to extended cable length
- Results in signal loss and no communication with the devices on the other end
- Solution:
  - Use a repeater
  - Use a different cable with greater distance support



Cable attenuation or signal loss occurs when a cable with more than the suggested length is used. For example, if a cable can transmit signals to 100 meters, you cannot use 150 meters cable and expect it to transmit the data. The extended cable length causes signal loss, known as cable attenuation. Sometimes, you need to extend the antenna with a specific cable length. When this cable is extended, there is an issue of signal loss. To work with this problem, you can use a repeater or use a different cable with greater distance support.

# RF Attenuation/Signal Loss

- Occurs due to various obstacles:
  - Concrete walls
  - Wooden doors
- Can be increased by:
  - Boosting the wireless router's signals
  - Using a range extender or repeater
  - Adjusting the antennas
  - Placing the wireless router on a different location
  - Raising the wireless router



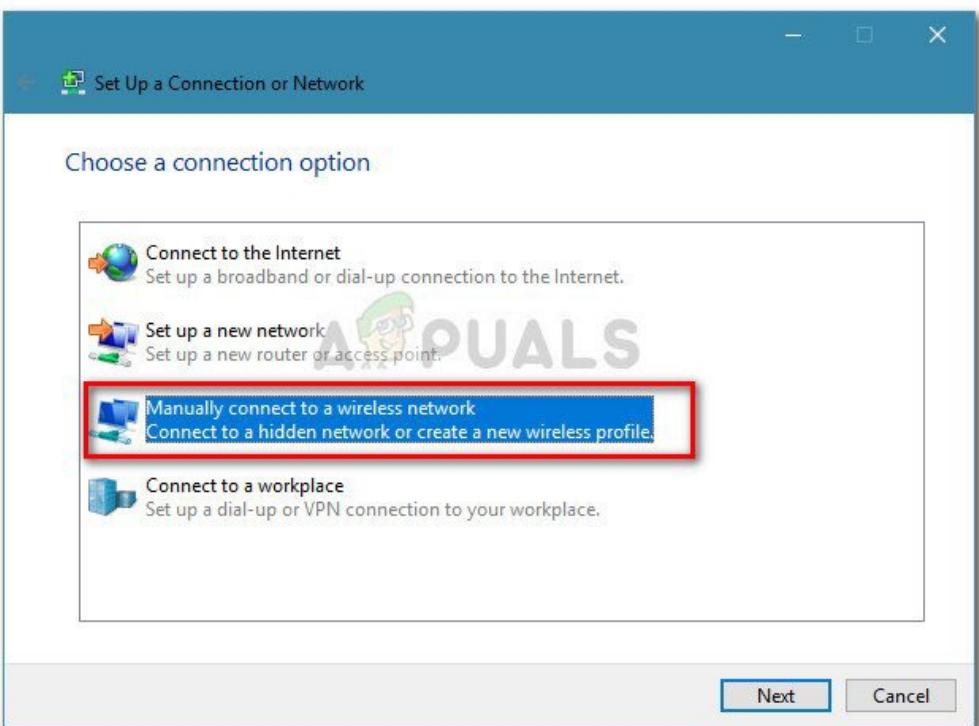
Signal loss can occur due to various reasons. There can be obstacles or even a wireless client located far away from the wireless router. Have you ever wondered why getting low wireless signals even though you are in the next room to the wireless router? Well, there are reasons. Obstacles like concrete walls and wooden doors cause signal loss – if the wireless signals are received in clear sight, the signal strength is much higher.

To increase the signal strength, you can:

- Boost the signals from the wireless router
- Install a wireless range extender or repeater – this helps as it can boost the signals into the dead zones
- Adjust the antennas – incorrect placement of antennas is a major issue. Wireless network performance can be improved with horizontal and vertical antenna placement.
- Place the wireless router on a different location – move it to a central location so that the signals can be broadcasted to all corners
- Raise the wireless router – this can be done for the clear sight visibility and better range to the wireless devices

# Wrong SSID

- Is outcome when you have to manually type the SSID
- Is case-sensitive – must be entered as defined
- Is the outcome of spelling errors



When you want to connect to a wireless network, you attempt to connect first. To do this, you need to find a wireless network. You scan through the available wireless networks. It is a simple method used to connect to a wireless network.

However, let's assume that the wireless network name is not visible – the administrator has disabled the SSID broadcast. You will need to add the wireless network manually. In this process, you need to provide the correct name for the wireless network. The wireless network name is case-sensitive. There is a spelling error in most cases, or you unknowingly type the wrong name. For example, you did not know that wireless network names are case-sensitive. Instead of MyWiReLeSs, you type mywireless. This will not work.

# Incorrect Passphrase

- Is an error generated due to an incorrect password being entered to connect to a wireless network
- Displays the following error:

“The network security key isn’t correct. Please try again.”



To connect to a wireless network, you typically need a password, which is not required if someone has left an open wireless network. If the password is incorrect, you are flashed with the following message:  
“The network security key isn’t correct. Please try again.”

Password protection is the security mechanism used by wireless networks.

# Encryption Protocol Mismatch

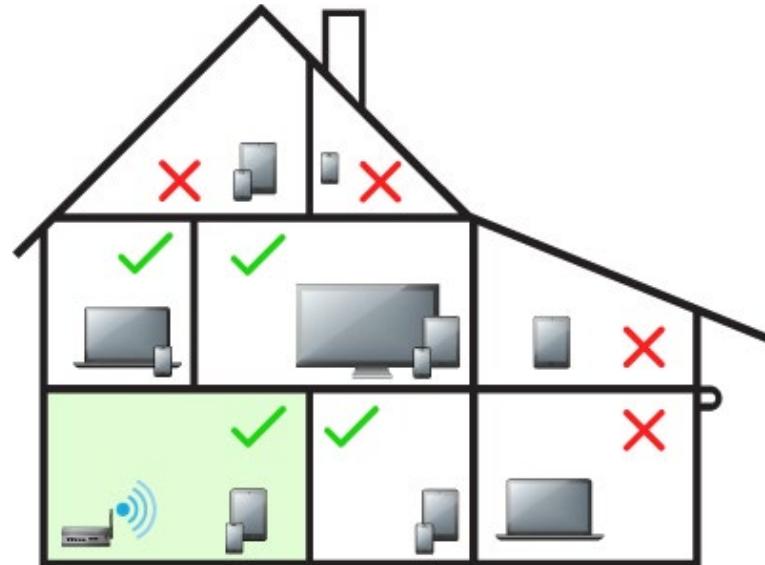
- Occurs when client and wireless routers are configured with different encryption protocols
- Prevents the client from connecting to the wireless network
- Can be solved by ensuring the client and wireless router use the same encryption protocol



For the wireless clients to connect to the wireless router, they need to use the same encryption protocol. The communication needs to be encrypted and decrypted using the same encryption method. If both are configured with different encryption protocols, communication cannot occur. For example, if you need to communicate with someone, both need to speak the same language, be it English or French. If one is speaking French and another one is speaking English, it is obvious that there will be communication failure. The same scenario works with the encryption protocols, preventing communication between the wireless client and the wireless router. The easiest solution is to configure both of them to use the same encryption protocol.

# Insufficient Wireless Coverage

- Is primarily due:
- To the wireless router placement
- To size of the facility
- To the antenna placement
- Can cause signal drops and client connectivity issues
- Can be overcome by wireless extender or repeater



You have already learned about the issues of insufficient wireless coverage. It can occur due to:

- To the wireless router placement
- To the size of the facility
- To the antenna placement

There can be an impact on the signals or connectivity due to these reasons.

You may have to change the wireless router placement, but it may not be possible in all scenarios. For example, if the wireless router is connected to the DSL line, you may not be able to move the wireless router.

If the facility is large, you can use wireless extenders or repeaters to extend the wireless signals.

# Captive Portal Issues

- Can be an issue when devices without Web browsers need to connect to a wireless network
- May pose a challenge in the existing network

**Example Captive Portal**

Welcome!  
Please enter your credentials to connect.

Username:

Password:

Access Code:

Terms and Conditions

1. The owner and operator ("Owner") of this computer network ("the Service") reserves the right to discontinue the Service at any time.

I agree to the Terms and Conditions

Captive portals are applications that need to be browsed using a Web browser. It becomes an issue with a wireless device that does not have a Web browser. In such a scenario, the wireless device cannot be authenticated with the captive portal and use the wireless network.

Another issue can be integrating the captive portal into the existing authentication schema on the network. There can be various issues, such as using an older authentication schema that is not available or easily integrated with the captive portal.

# Client Disassociation Issues

- Can occur due to several reasons:
  - Idle / Session timeout
  - Wireless network configuration changes
  - Authentication timeout
  - Channel change
  - Wireless router reboot

There can be several reasons for client disassociations.

Idle or session timeout

Wireless network configuration changes

Authentication timeout

Channel change

Wireless router reboot

In most cases, the wireless clients reassociate themselves with the wireless router. For example, the wireless clients are disassociated if you reboot the wireless router. However, as soon as the wireless router is back online, they are again associated.



# Summary

- Specifications and limitations
- Considerations
- Common issues



That's the end of the lesson.

Here we covered:

- Specifications and limitations
- Considerations
- Common issues

A person is sitting at a desk in a dimly lit room, looking at a computer screen. The background is dark and slightly blurred.

*NEXT TOPIC*

---

## TROUBLESHOOT GENERAL NETWORKING ISSUES

---

# 5

---

# Troubleshooting Networking Issues

- 1 — Welcome to the 5 lesson of Module 5. In this lesson, you will learn about the:
  - 2 — Troubleshooting Networking Issues
-

# Agenda

- Considerations
- Common Issues



Hi, welcome to COMPTIA Network+ Course

In this lesson, we will talk about:

- Considerations
- Common Issues



A photograph of two women in an office setting. On the left, a woman with blonde hair, wearing a red patterned blouse, holds a white paper and a pen, smiling at the camera. On the right, another woman with dark hair, wearing a dark blazer over a light shirt, also smiles. They appear to be in a professional environment, possibly reviewing documents together.

*TOPIC 1*

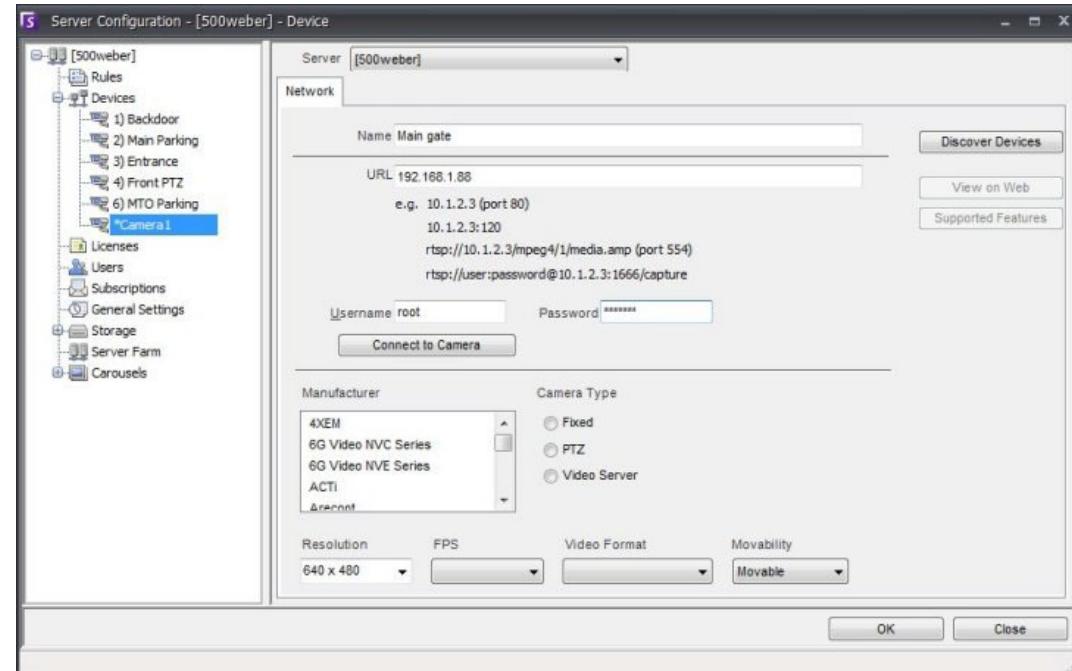
---

# CONSIDERATIONS

---

# Device Configuration Review

- Is critical for a device or an application to function
- Can cause issues if not done properly



Several devices are part of a network. Without appropriate configuration, these devices may not function properly. For example, you can install a firewall on the edge of a network. However, if the firewall is not configured properly, it will serve no purpose. It will not filter the traffic, which is its main purpose.

A misconfigured or inappropriately configured device can cause several issues. It might get exploited or become part of an attack, or it may even cause network issues. For example, a misconfigured firewall can be advantageous for attackers. They can leverage the misconfiguration and exploit them.

# Routing Tables

- Are used to forward packets to different networks
- Are used by the router to forward packets to the correct destination
- Can be updated by connected networks, static, and dynamic routing
- Can stop communication between networks if not updated

```
[root@fedora10 ~]# netstat -nr
Kernel IP routing table
Destination     Gateway         Genmask        Flags   MSS Window irtt Iface
60.49.199.72    0.0.0.0        255.255.255.248 U        0 0          0 eth1
172.16.163.0    172.16.160.1  255.255.255.0   UG      0 0          0 eth0
172.16.162.0    172.16.160.1  255.255.255.0   UG      0 0          0 eth0
172.16.161.0    172.16.160.1  255.255.255.0   UG      0 0          0 eth0
172.16.160.0    0.0.0.0        255.255.255.0   U        0 0          0 eth0
172.16.167.0    172.16.160.1  255.255.255.0   UG      0 0          0 eth0
172.16.166.0    172.16.160.1  255.255.255.0   UG      0 0          0 eth0
172.16.165.0    172.16.160.1  255.255.255.0   UG      0 0          0 eth0
172.16.164.0    172.16.160.1  255.255.255.0   UG      0 0          0 eth0
172.16.170.0    172.16.160.1  255.255.255.0   UG      0 0          0 eth0
172.16.169.0    172.16.160.1  255.255.255.0   UG      0 0          0 eth0
172.16.168.0    172.16.160.1  255.255.255.0   UG      0 0          0 eth0
169.254.0.0     0.0.0.0        255.255.0.0    U        0 0          0 eth0
169.254.0.0     0.0.0.0        255.255.0.0    U        0 0          0 eth1
0.0.0.0          60.49.199.73  0.0.0.0       UG      0 0          0 eth1
[root@fedora10 ~]#
```

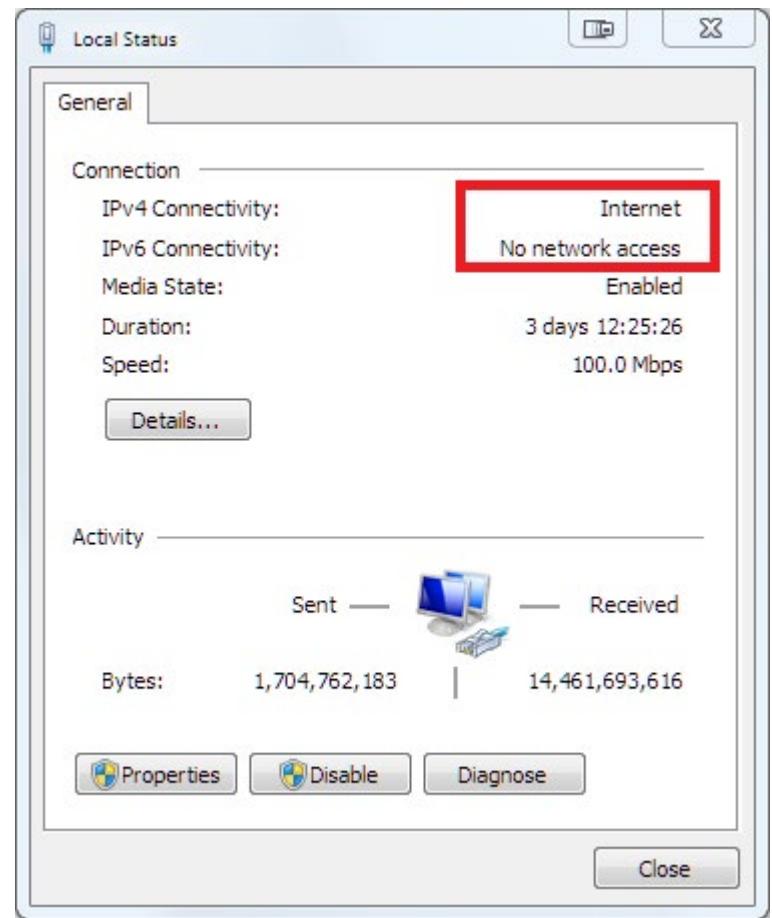
Routing tables contain the routes. When a packet needs to go out of a subnet or a network, it will not find its destination without the routing table. If a packet is sent within the same subnet, it is directly forwarded to the destination system. However, if the packet has to go out of a subnet, it needs to use a router, which uses the routing tables and the packet's interface. The router reads the destination address from the packet and uses the routing table to send the packet. The routing table contains only the known routes by the router.

You can have several routes added to the routing table, which builds dynamically when installing a system. However, you can also add static routes and make them persistent, which means that the persistent routes will exist even after the system reboot.

If you need to send a packet to a system, but there is no route, then the packet cannot be sent.

# Interface Status

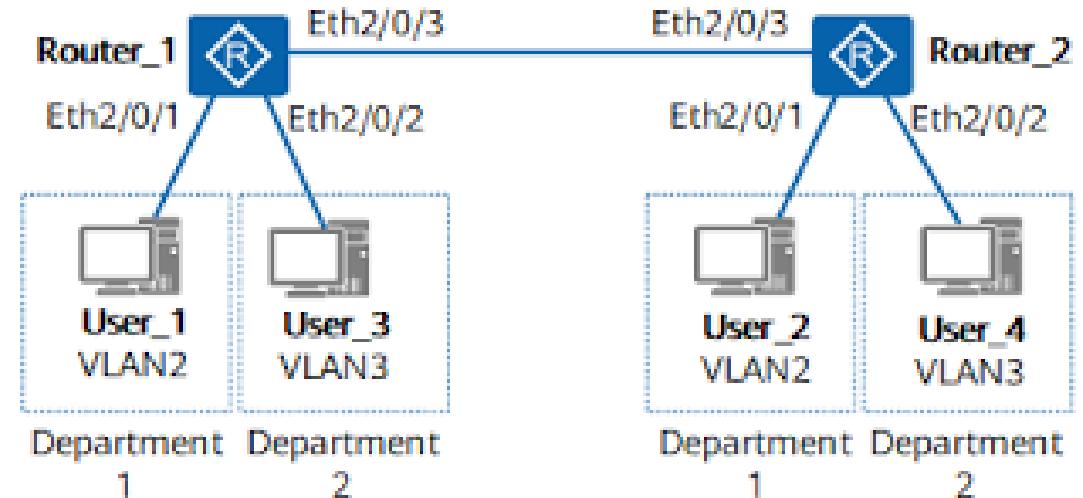
- Displays the network status
- Can also display the if there is a connectivity break



Each network interface must be monitored. Operating systems and network devices have tools or commands that can help you monitor the network interface. With the monitoring, you can verify the traffic flowing in and out of the interface and overall interface status and detect any connectivity breaks or issues. For example, if you use Windows, you can get into the network interface properties and check the connectivity and the traffic status.

# VLAN Assignment

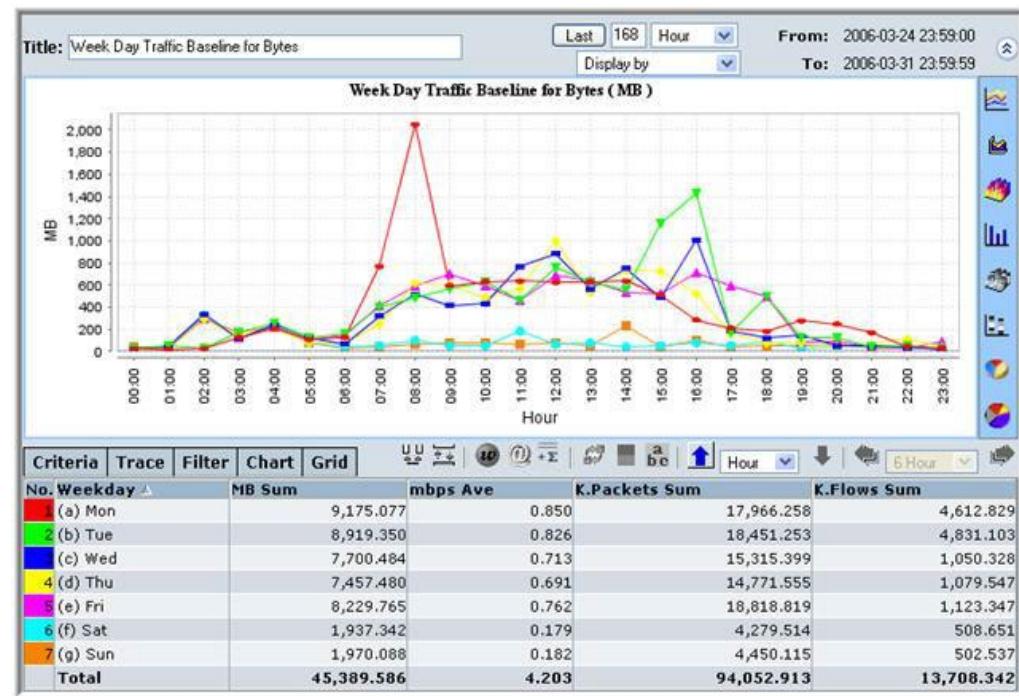
- Is to a group of systems and users to be in a small part of a large network
- Helps to restrict traffic in a limited part of the network



A VLAN is a smaller portion of a larger network. You can have hundreds of VLANs in a large network. Using VLAN assignment, you put a group of systems and users in a small portion of a network. With the VLAN assignment to the users and systems, you can restrict traffic within the same portion of the network. This helps you control the flow of information. For example, if a specific VLAN needs to be restricted from other users, you can use access control lists to restrict access.

# Network Performance Baselines

- Are created to detect the performance issues



A network performance baseline helps you determine the optimal performance. You can continue monitoring the network, collecting and analyzing information, and comparing them with the network performance baseline. You may even find some surprising information about where the bandwidth is getting choked or there is some strange traffic originating from a specific server.

When you make changes to the network, you should update the network performance baselines. The old one will be of no use because it will not monitor and compare the new changes in the network. With the comparison, you can locate areas of the network that may need improvements.



***TOPIC 2***

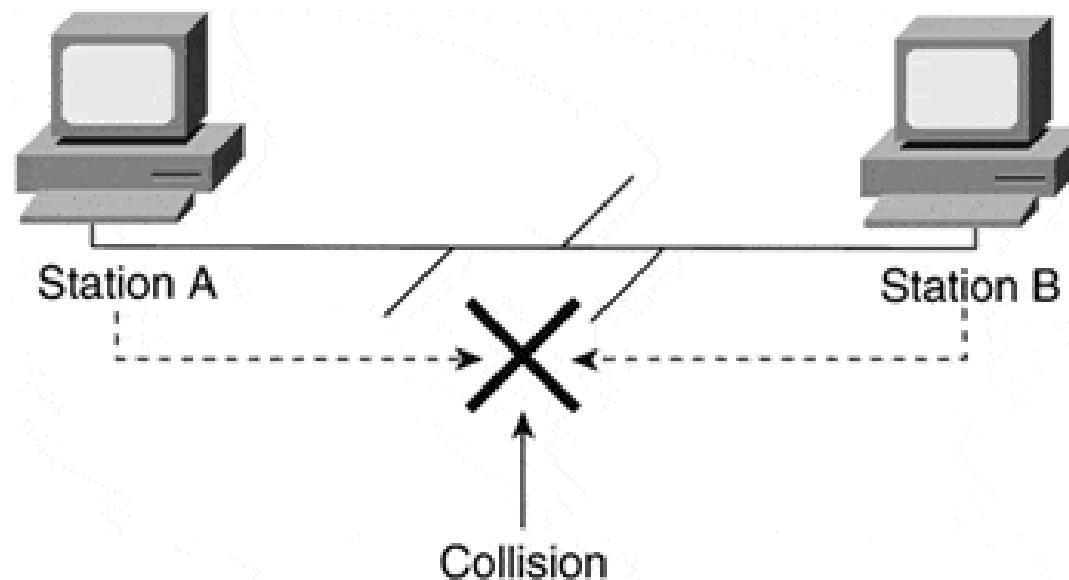
---

# COMMON ISSUES

---

# Collisions

- Occurs when two systems (or more) attempt to transmit the signal simultaneously
- Can be handled with Carrier Sense Multiple Access with Collision Detection (CSMA/CD)

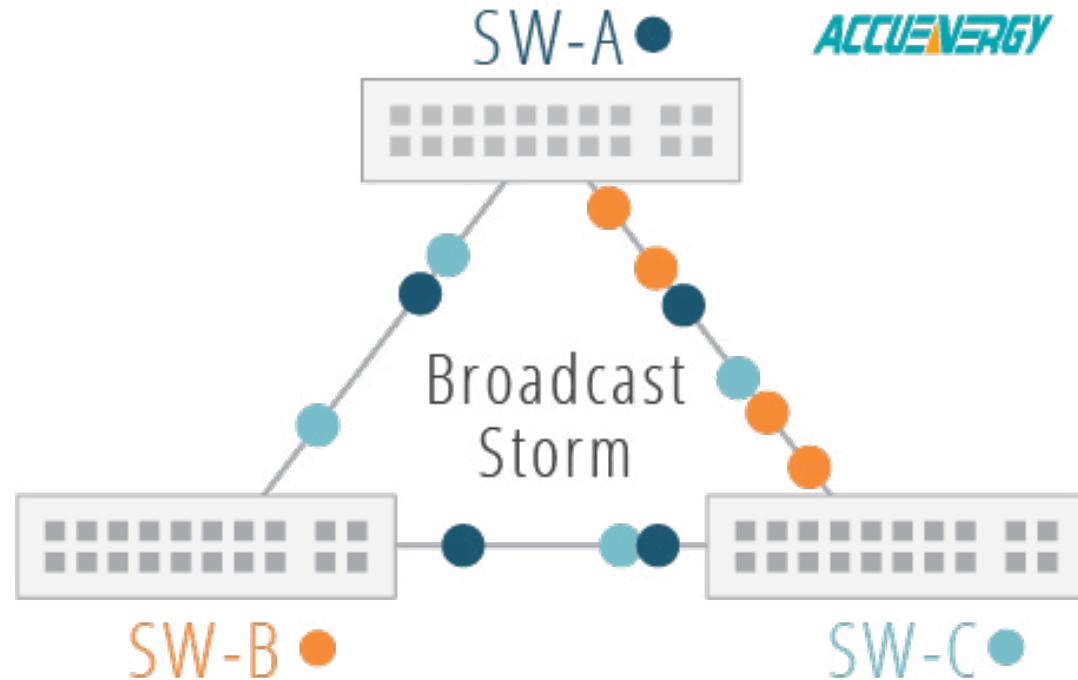


Collisions cause network performance bottlenecks. Collisions occur when several computers, or even two, start transmitting information over the network simultaneously. Collisions are common when systems are connected to a hub, which cannot prevent collisions. Collisions occur at the Physical layer of the OSI model – the physical layer because systems share a single device.

The Ethernet networks use Carrier Sense Multiple Access with Collision Detection (CSMA/CD) to resolve the collisions on the network.

# Broadcast Storm

- Is a high volume of packets sent over a network
- Can degrade the network performance



ACCUEENERGY

A broadcast storm is a high volume of packets that flood the network within a limited time. The packets have to travel through the switches, which may make handling the flood of broadcast packets difficult. This eventually impacts the network performance. The broadcast storm consumes the network resources, preventing network devices from catering to legitimate requests.

# Duplicate MAC Address

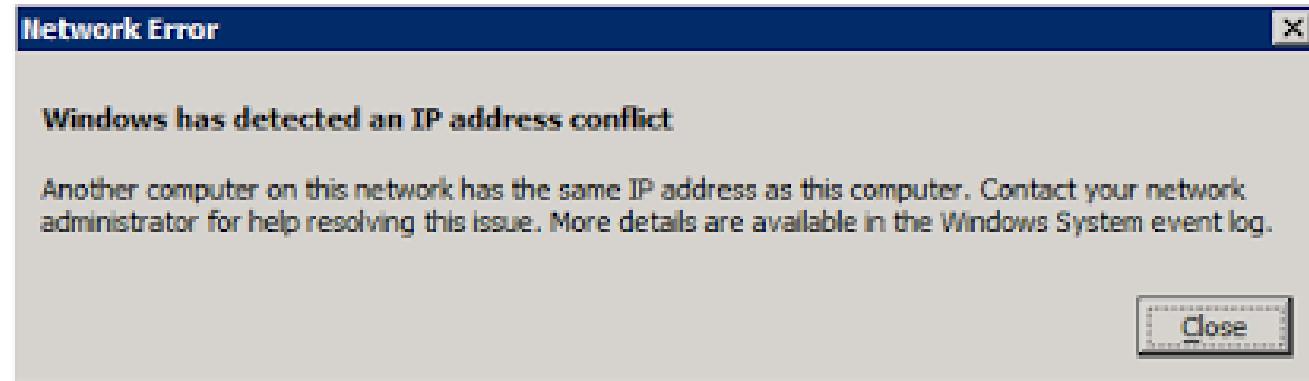
- Occurs because of MAC Spoofing attack

IP	NetBIOS group	Manufacturer	MAC address
192.168.6.51	\\fa\\fa\\fa\\fa\\f	Ubiquiti Networks Inc.	44:D9:E7:70:4E:F5
192.168.6.58		Ubiquiti Networks Inc.	44:D9:E7:70:4E:F5
192.168.6.59		Ubiquiti Networks Inc.	44:D9:E7:70:4E:F5
192.168.6.77		Ubiquiti Networks Inc.	44:D9:E7:70:4E:F5
192.168.6.82		Ubiquiti Networks Inc.	44:D9:E7:70:4E:F5
192.168.6.89		Ubiquiti Networks Inc.	44:D9:E7:70:4E:F5
192.168.6.90		Ubiquiti Networks Inc.	44:D9:E7:70:4E:F5
192.168.6.102		Ubiquiti Networks Inc.	44:D9:E7:70:4E:F5
192.168.6.108		Ubiquiti Networks Inc.	44:D9:E7:70:4E:F5
192.168.6.122		Ubiquiti Networks Inc.	44:D9:E7:70:4E:F5
192.168.6.127		Ubiquiti Networks Inc.	44:D9:E7:70:4E:F5
192.168.6.147		Ubiquiti Networks Inc.	44:D9:E7:70:4E:F5
192.168.6.157		Ubiquiti Networks Inc.	44:D9:E7:70:4E:F5
192.168.6.180		Ubiquiti Networks Inc.	44:D9:E7:70:4E:F5
192.168.6.182		Ubiquiti Networks Inc.	44:D9:E7:70:4E:F5
192.168.6.189		Ubiquiti Networks Inc.	44:D9:E7:70:4E:F5
192.168.6.245		Ubiquiti Networks Inc.	44:D9:E7:70:4F:21
192.168.6.251		Ubiquiti Networks Inc.	44:D9:E7:70:4E:F5

A MAC address is a physical address of a network adapter embedded in it. MAC address is globally unique, which means two network adapters cannot have the same MAC address. However, a MAC address can be spoofed. An attacker can find a legitimate MAC address by footprinting a device or several devices on a network and spoofing its MAC address to his device to gain access to the network resources. For example, let's say that a wireless network whitelists devices based on their MAC addresses. When the attacker spoofs a legitimate device's MAC address, the attacker can access the wireless network. With this, the attacker can communicate with the other devices on the wireless network.

# Duplicate IP Address

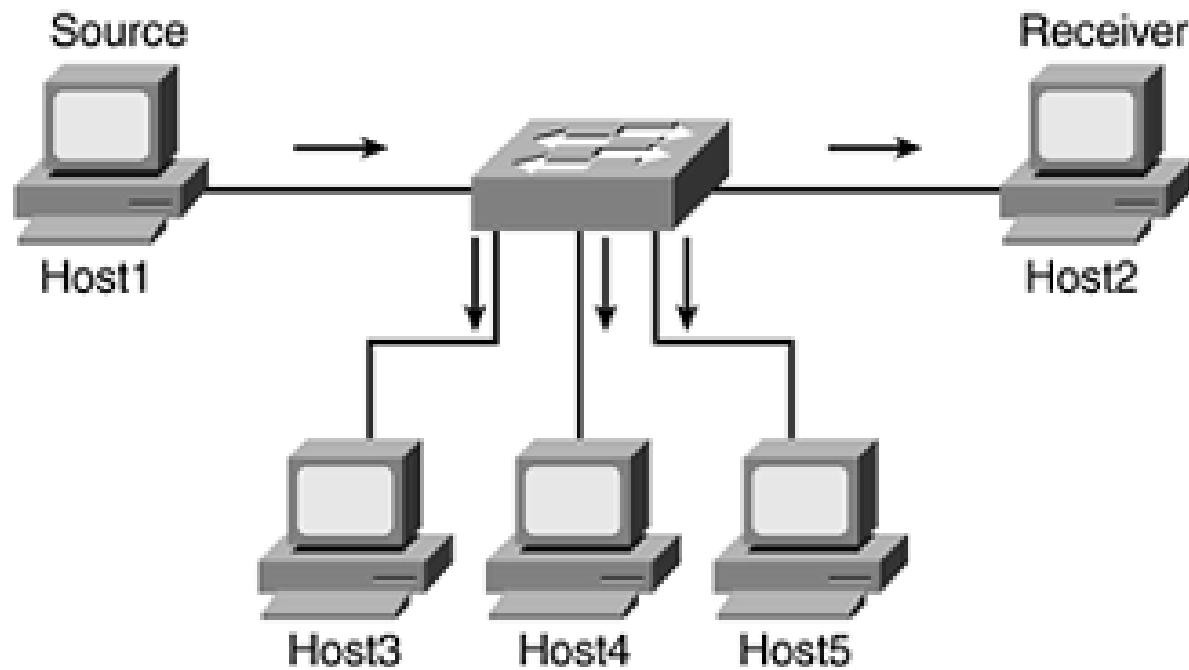
- Is an issue where two systems are assigned the same IP address
- Takes place usually because of one system having a dynamic IP and another one with static IP



On a network, devices and systems must have a unique IP address. If two devices or systems have the same IP address, the duplicate IP address occurs. This typically happens when one device or system receives IP addresses from the DHCP server, and another has statically assigned IP addresses. The static IP addresses must be added to the exclusions to resolve this issue. The excluded IP addresses will not be leased to the clients when you do this.

# Multicast Flooding

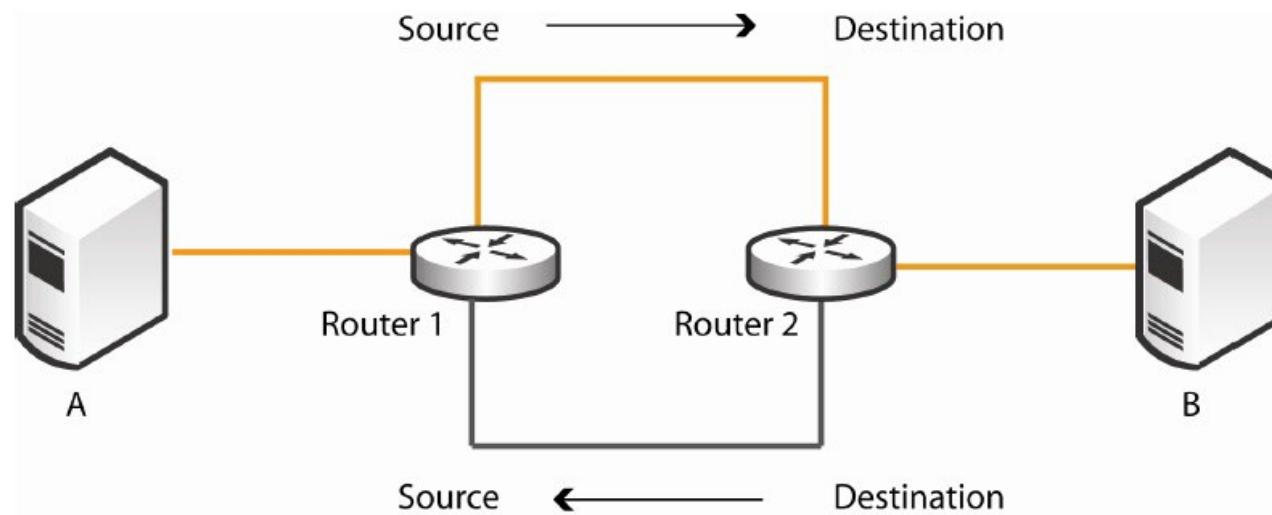
- Occurs in VLANs
- Takes place when a switch sends out a multicast packet to all ports



A multicast flood occurs when a switch receives a multicast packet. The switch needs to forward the multicast packet to its destination, but it does not know to whom this IP address belongs. The switch sends the packet to all ports to send this multicast packet. This causes the multicast flood. To prevent the multicast flood, switches can be configured to prevent the forwarding of the multicast packets to all ports. Rather, switches can be configured to send multicast packets for an unknown destination to a specific port.

# Asymmetrical Routing

- Is when a packet uses two different paths – one for reaching the destination and another one for returning to source

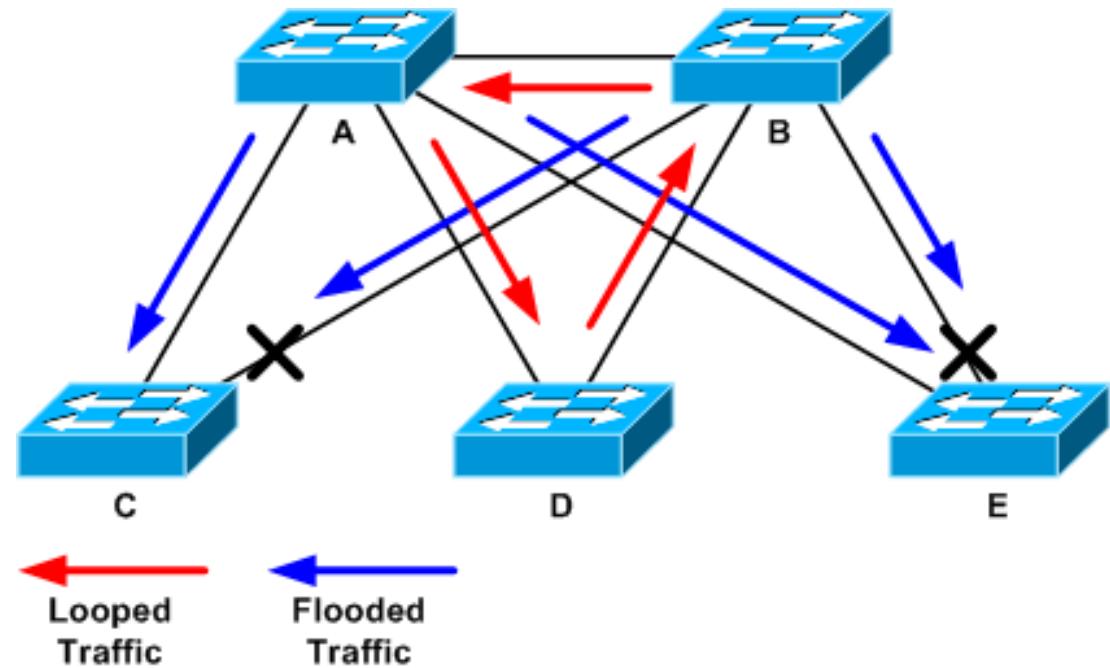


When a packet travels, it travels on a single path – traveling to the destination and coming back on the same path to the source from it started. However, in asymmetrical routing, the packet takes one path to the destination but returns using a different path. The biggest drawback of asymmetrical routing is that it may cause the packets to arrive incorrectly.

The solution to prevent asymmetrical routing is by fixing the routing so that the packets leave and come back using the same path.

# Switching Loops

- Occurs between:
  - Two switches
  - Two ports on the same switches
- Creates a broadcast storm



Switch loop can occur due to two reasons:

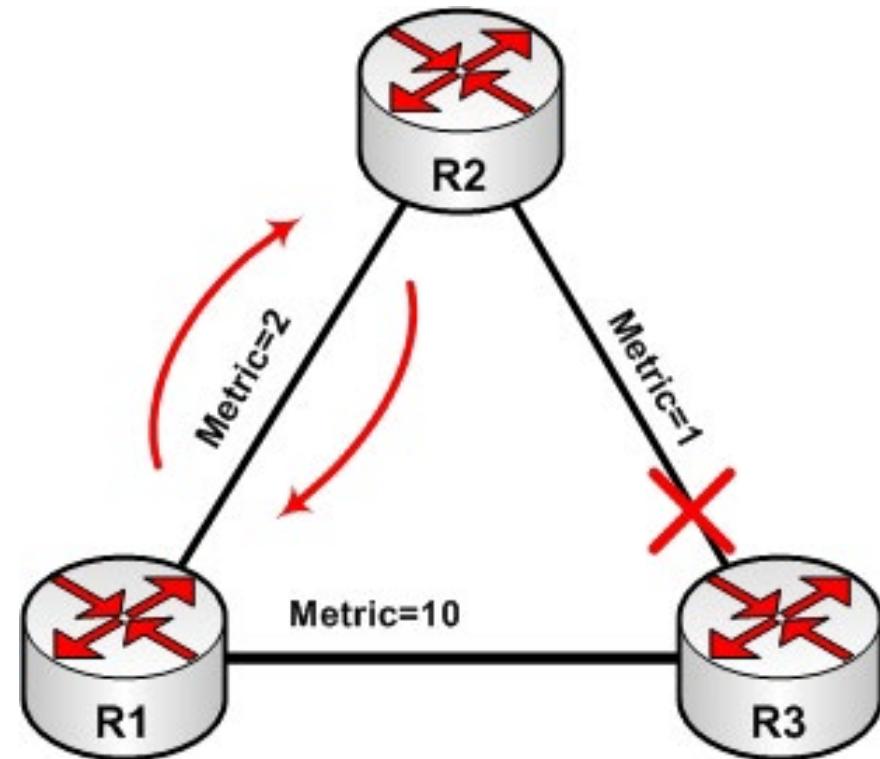
- More than one connection between two switches
- Two ports on a switch connected

The outcome of the switching loop is a broadcast storm. It can even cause a multicast storm if multicast packets are received and then forwarded by a switch. A switching loop is created because the Layer 2 header does not contain the time to live or TTL field. Therefore, if a packet enters the looped switches or ports, it goes into an infinity loop.

You should use physical loops using either shortest path bridging (SPB) or the spanning tree protocols (STP) to prevent a switching loop.

# Routing Loops

- Occurs due to the cyclical entries in the routers
- Cause the packets to go back and forth between two routers
- Can be preventing by limiting the hop count

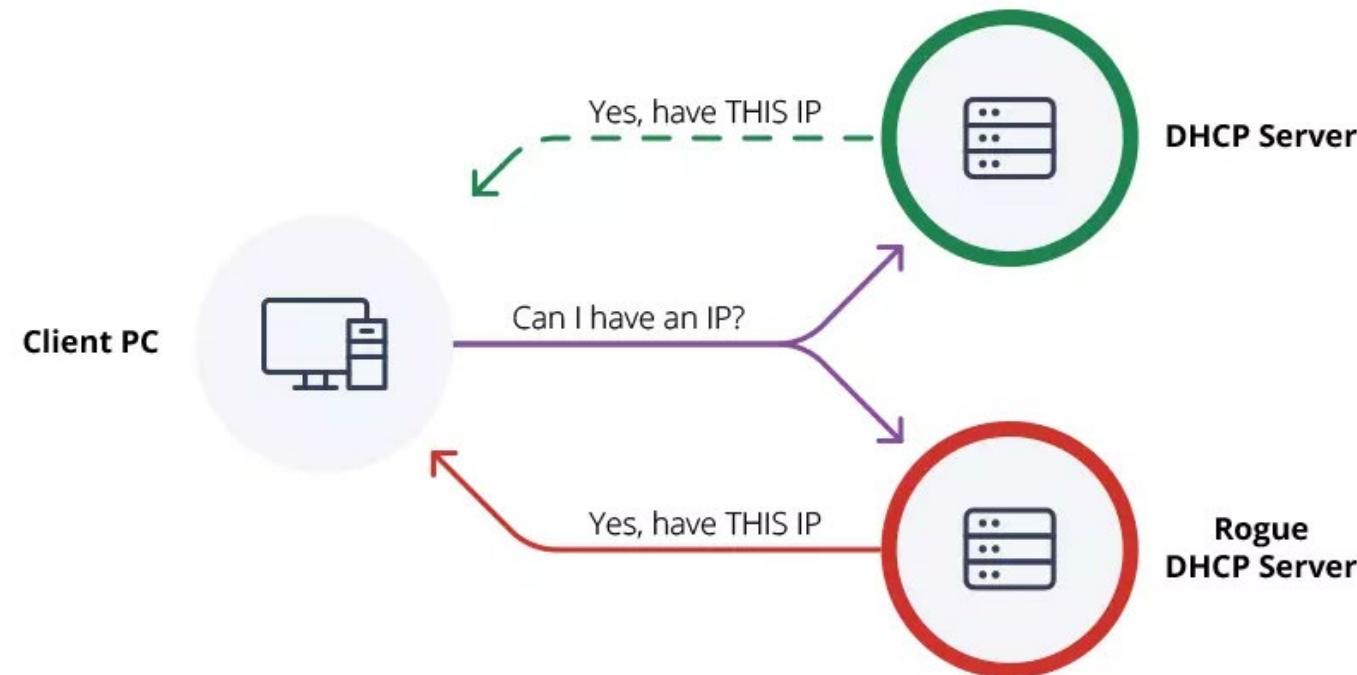


A routing loop is the result of cyclical entries in a routing table. A routing loop occurs when routers keep forwarding the packets to each other, considering using the best route. For example, router1 needs to send the packets to router3. It forwards the packets to router2 as it is considered the best route. When router2 receives the packets, it checks its routing table and finds that router1 is the best route to send the packets to router3. In reality, the packets don't reach router3 because router1 sends it to router2, which sends it back to router1.

To prevent the routing loops from occurring, you should limit the maximum hop count.

# Rogue DHCP Server

- Is an unauthorized DHCP server that releases IP addresses on a network
- Can be used to initiate an attack

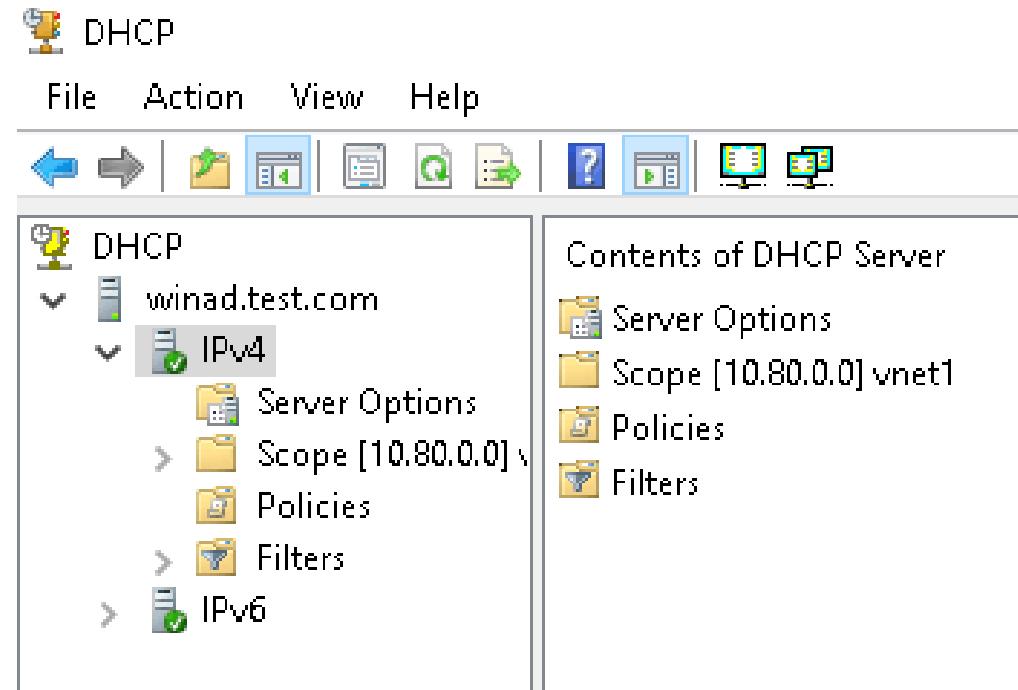


A rogue DHCP server is just an unauthorized server leasing IP addresses to the network clients. It can be accidentally installed by a user, who may be setting up a small testing environment, but such scenarios are rare. It can be set up by a person who can use it to conduct a man-in-the-middle attack.

There are several methods to prevent a rogue DHCP server in a network. First of all, if there are several systems with IP address conflicts on a network, you can very well assume that there is a rogue DHCP server. In a Windows environment, you must authorize every DHCP server. Finally, the most secure solution enables DHCP snooping on the managed switches. The DHCP server needs to be plugged into a trusted port. If DHCP responses are coming from an untrusted port, they are ignored.

# DHCP Scope Exhaustion

- Occurs when a DHCP scope runs out of IP addresses
- Can be handled by decreasing the lease time or increasing the scope

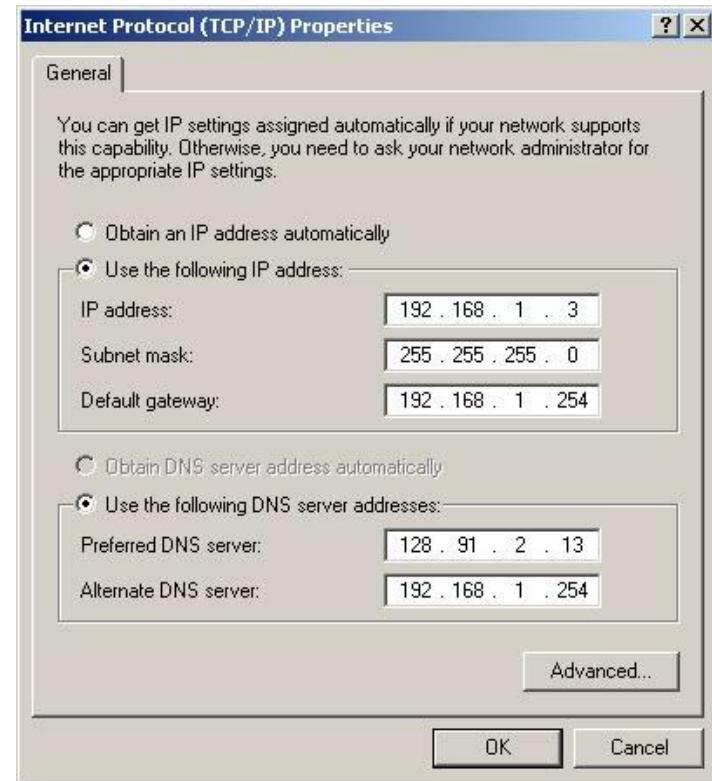


A DHCP can contain various IP scopes used to lease IP addresses to the client. Each scope can be configured with a specific number of IP addresses. When all these IP addresses are leased to the clients, and no more IP addresses are available to lease, then the DHCP scope is exhausted.

To handle the DHCP scope exhaustion, you can increase the number of IP addresses in the scope. However, if you have already done that, there is no other option but to decrease the lease time.

# IP Setting Issues

- Can be due to
  - Incorrect gateway
  - Incorrect subnet mask
  - Incorrect IP address
  - Incorrect DNS



IP setting issues generally occur when manually assigning a static IP address to a system. You may enter the incorrect information for:

- Gateway
- Subnet mask
- IP address
- DNS

All this information, if dynamically assigned, is passed on to the system via the DHCP server. If several users face any of these issues, you should check the DHCP settings passed into the IP addresses.

# Missing Route

- Can be due to:
  - Broken topology
  - Error in static route
  - Error in routing protocol configuration

```
PC>ping 10.0.0.3

Pinging 10.0.0.3 with 32 bytes of data:

Reply from 20.0.0.1: Destination host unreachable.

Ping statistics for 10.0.0.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

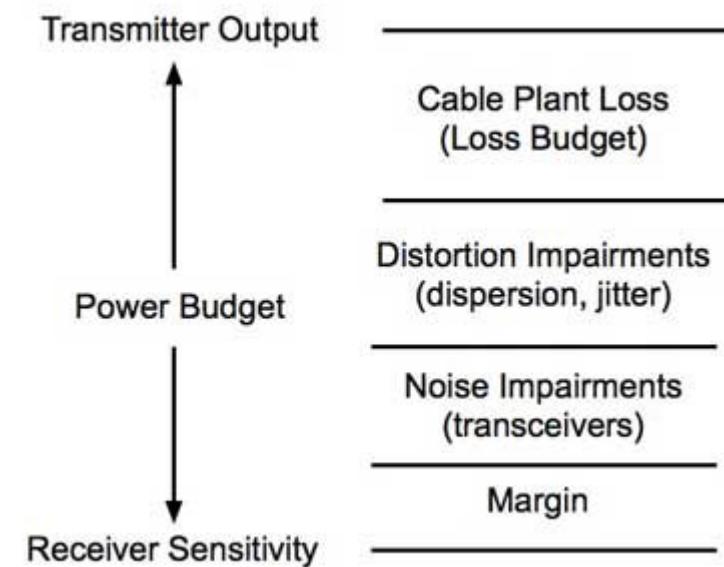
A missing route can be due to several reasons. It could be broken topology, which may occur due to a faulty backbone or a major network issue. It could also be an error in the static route that was manually entered. It could also be due to the error in routing protocol configuration.

When there is a missing route, it prevents the data from reaching its destination. Depending on the reason for the missing route, you have to rectify it. For example, if it is a problem with the static route, you have to fix it by deleting it and adding a new one.



# Low Optical Link Budget

- Is due to:
  - Attenuation
  - Splice losses
  - Connector losses



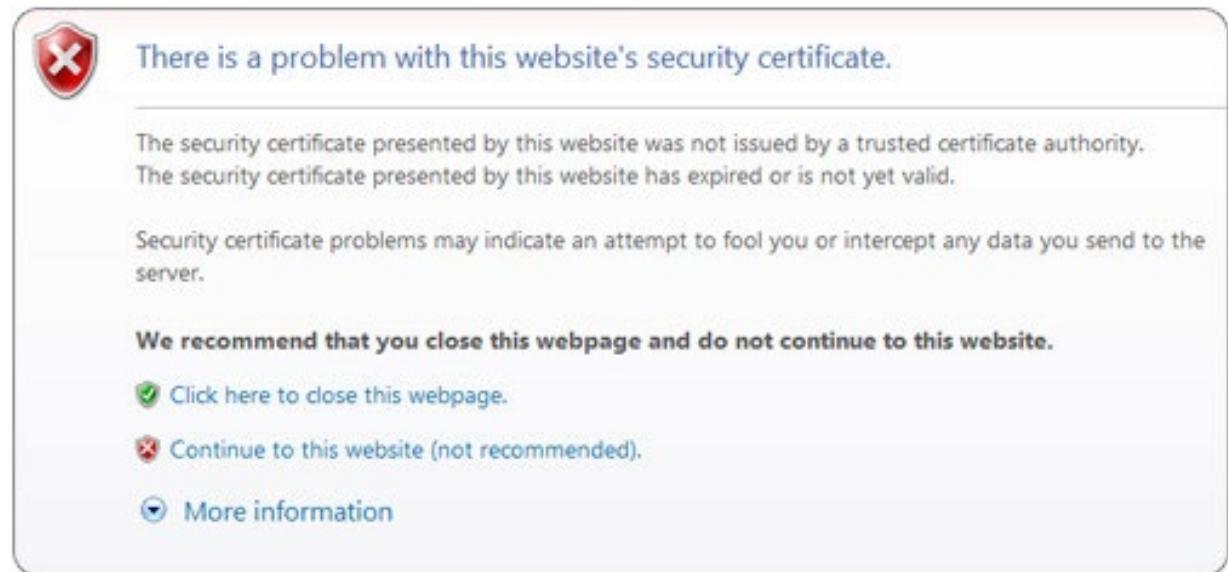
The low optical link budget is about the optical power budget of a fiber-optic link. The low optical link budget occurs due to several factors, such as:

- Attenuation
- Splice losses
- Connector losses

Ensure that you pay attention to these factors to fix the low optical link budget.

# Certificate Issues

- Occurs due to:
  - Expired certificates
  - Unsigned certificates
- Can be caused by:
  - Older web browser
  - Unsupported web browser



Sometimes you encounter a certificate issue when browsing a website, as displayed on the slide. This issue occurs due to either expired or unsigned certificates. An expired certificate is the one of which the validity has expired. An unsigned certificate is typically a self-signed certificate and is not signed by a certificate authority. Older versions or unsupported web browsers can also cause the certificate issue. To correct this issue, you should upgrade the existing version. An expired or unsigned certificate should be replaced with a valid certificate.

# Hardware Failure

- Can occur with different networking devices:
  - Hubs
  - Switches
  - Routers
  - Wireless Access Points (WAPs)
- Can be due to a component failure, such as RAM or CPU

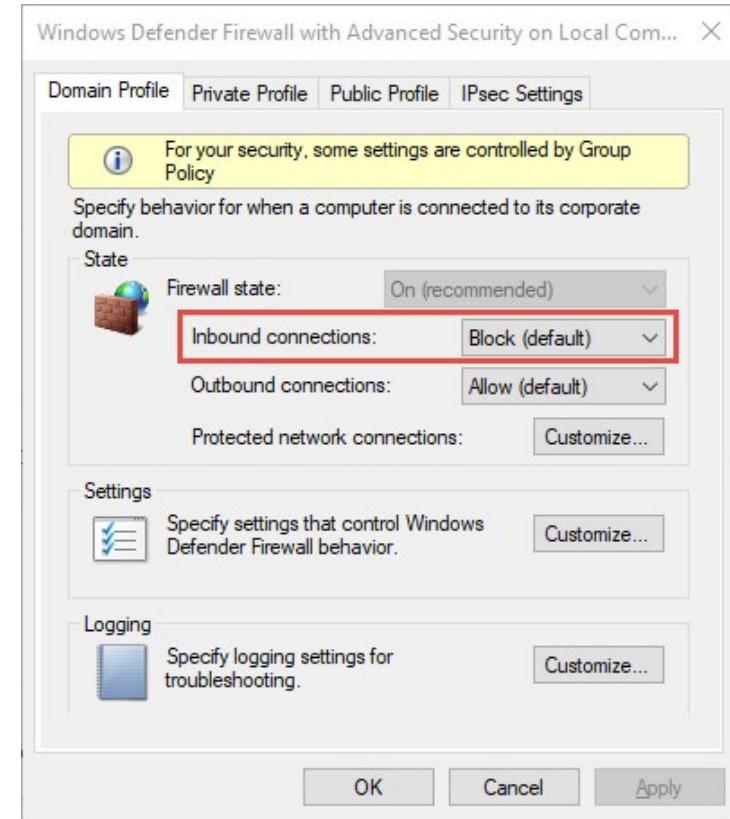


There can be several networking devices that can fail. Some key networking devices are hubs, switches, routers, and wireless access points (WAPs). The networking devices can be prone to different types of hardware failure – failed CPU, bad memory chips, or a non-functional network adapter.

To resolve a hardware issue, you should perform a hardware inspection. Most systems come with hardware inspection utilities that can detect a specific hardware malfunctioning.

# Host-based/Network-based Firewall Settings

- Are configured to prevent a system or a network
- Can be prone to different misconfigurations:
  - Blocking the ports and services that need to be opened
  - Open the ports and services that need to be blocked



A host-based or network-based firewall is designed to protect a system or a network. Its main purpose is to filter ingress and egress traffic. However, there can be several misconfigurations that can be done on these firewalls. For example, you keep the Deny All rule as the first rule, eventually blocking all incoming traffic. Misconfigurations can be of two types. The first one is that you block ports and services that need to be opened. The second one is that you open ports and services that must be blocked. Such misconfiguration will prevent a service from being functional. To resolve any misconfigurations, you need to consider the system or network security and then configure rules in the firewall.

# Blocked Services, Ports, or Addresses

The screenshot shows the Untangle Network configuration interface. The top navigation bar includes links for Dashboard, Apps, Config (selected), and Reports. Below the navigation is a secondary menu with Back to Config, Network (selected), and tabs for Interfaces, Hostname, Services, Port Forward Rules, NAT Rules, Bypass Rules, Filter Rules (which is highlighted with a red box), Routes, DNS Server, and DHCP.

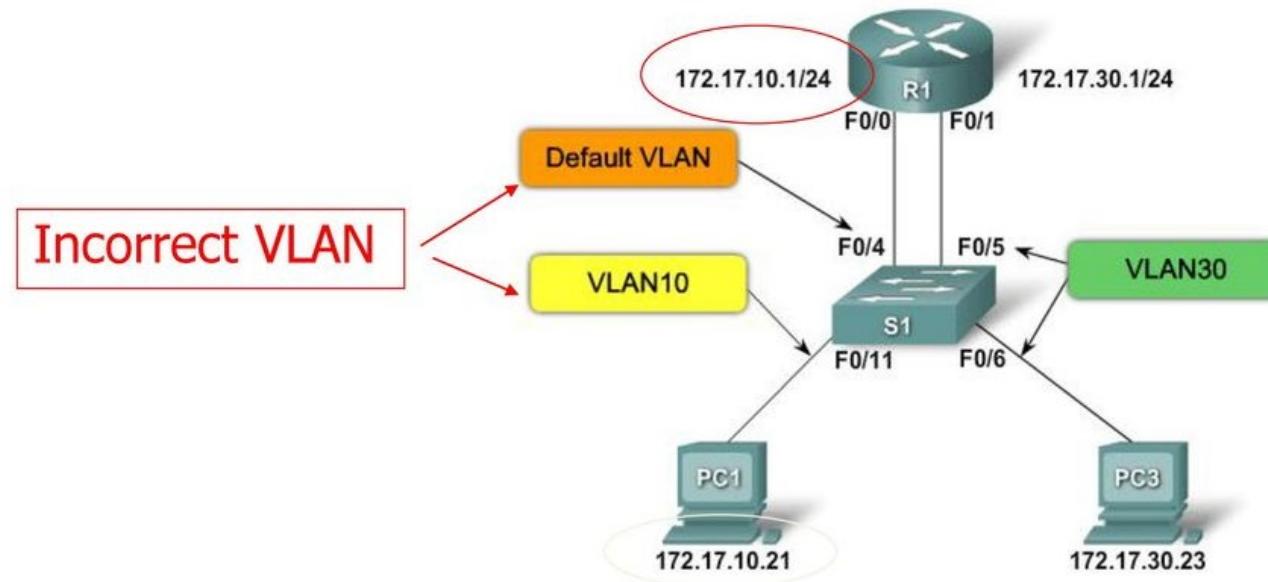
The main content area displays a table titled "Filter Rules". The table has columns for Rule Id, Enable, IPv6, Description, Conditions, Block, Edit, and Delete. There are two entries in the table:

Rule Id	Enable	IPv6	Description	Conditions	Block	Edit	Delete
new	<input checked="" type="checkbox"/>	<input type="checkbox"/>	block traffic from 65.50.1.25	Source Address ⇒ 65.50.1.25	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
new	<input checked="" type="checkbox"/>	<input type="checkbox"/>	block traffic to 65.50.1.25	Destination Address ⇒ 65.50.1.25	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

You block ports, services, and IP addresses using firewall rules. You must analyze your requirements and open or block a port, service, or IP address accordingly. If a port is blocked, let's say FTP port 21, and you have configured an FTP server on the system, the clients will not connect to it. The firewall will reject the traffic for port 21.

# Incorrect VLAN

- Is a VLAN to which a client connects while it intended to connect to a different VLAN
- Can occur due to the client connected to the wrong port on the switch

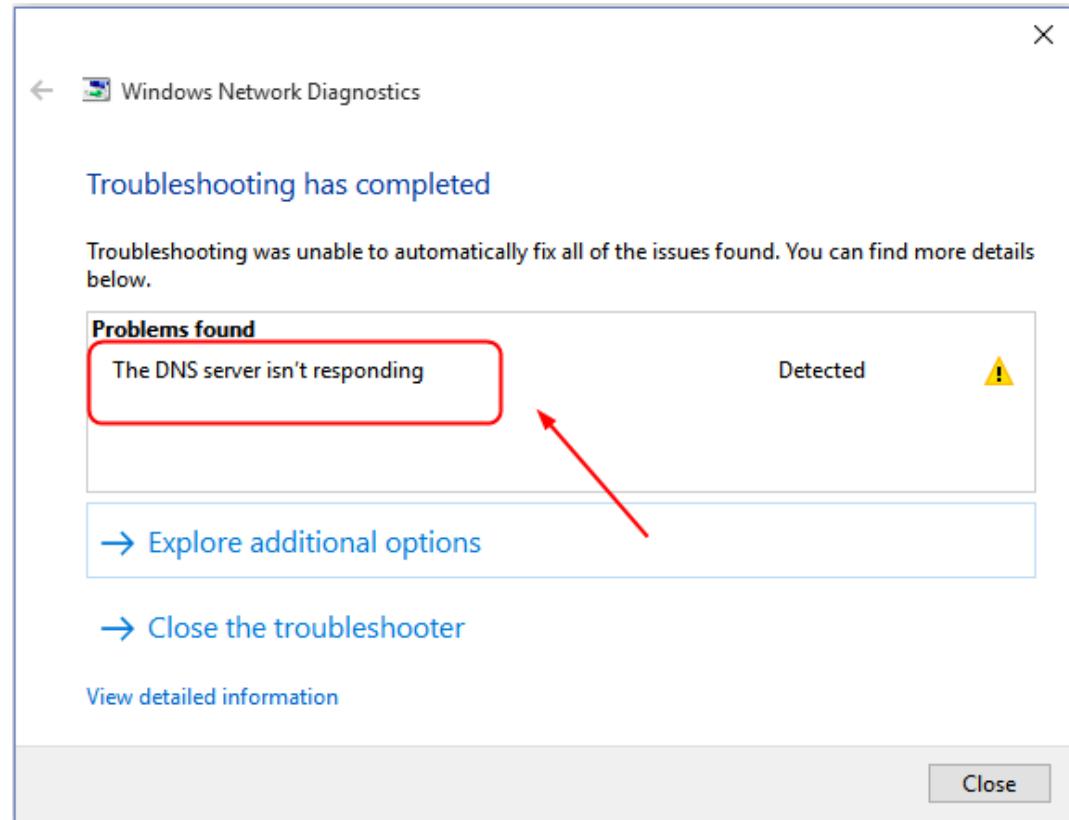


An incorrect VLAN issue occurs when a client system receives incorrect IP details from the DHCP server. The key reason behind this issue is that the client system is connected to a port configured with a different VLAN than the client was supposed to be connected to.

To resolve this issue, you should connect the client to the correct port on the switch.

# DNS Issues

- Can be due to
  - Incorrect IP configuration on a client device
  - Can be due to DNS server being unresponsive

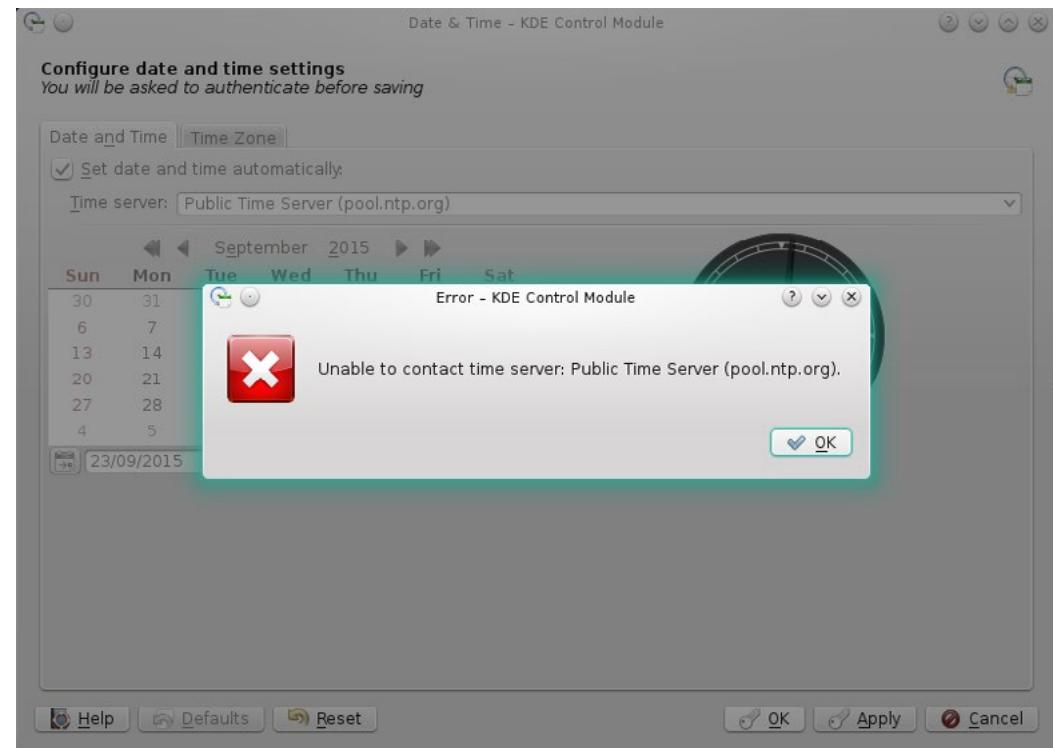


There can be several reasons for DNS issues. The first reason for a DNS issue is that the DNS name is incorrectly assigned via the IP configuration. If a client system is assigned an IP address via the DHCP server, it may have a wrong DNS server IP address. If you have assigned a static IP address, you may have incorrectly assigned a wrong DNS address. To resolve this, carefully verify the DNS assignment. The outcome is that the name resolution does not work.

It could also be possible that DNS is failing or having an issue due to which it becomes non-responsive. To resolve this issue, you should review the logs for any issues. Sometimes just restarting the server solves the problem.

# NTP Issues

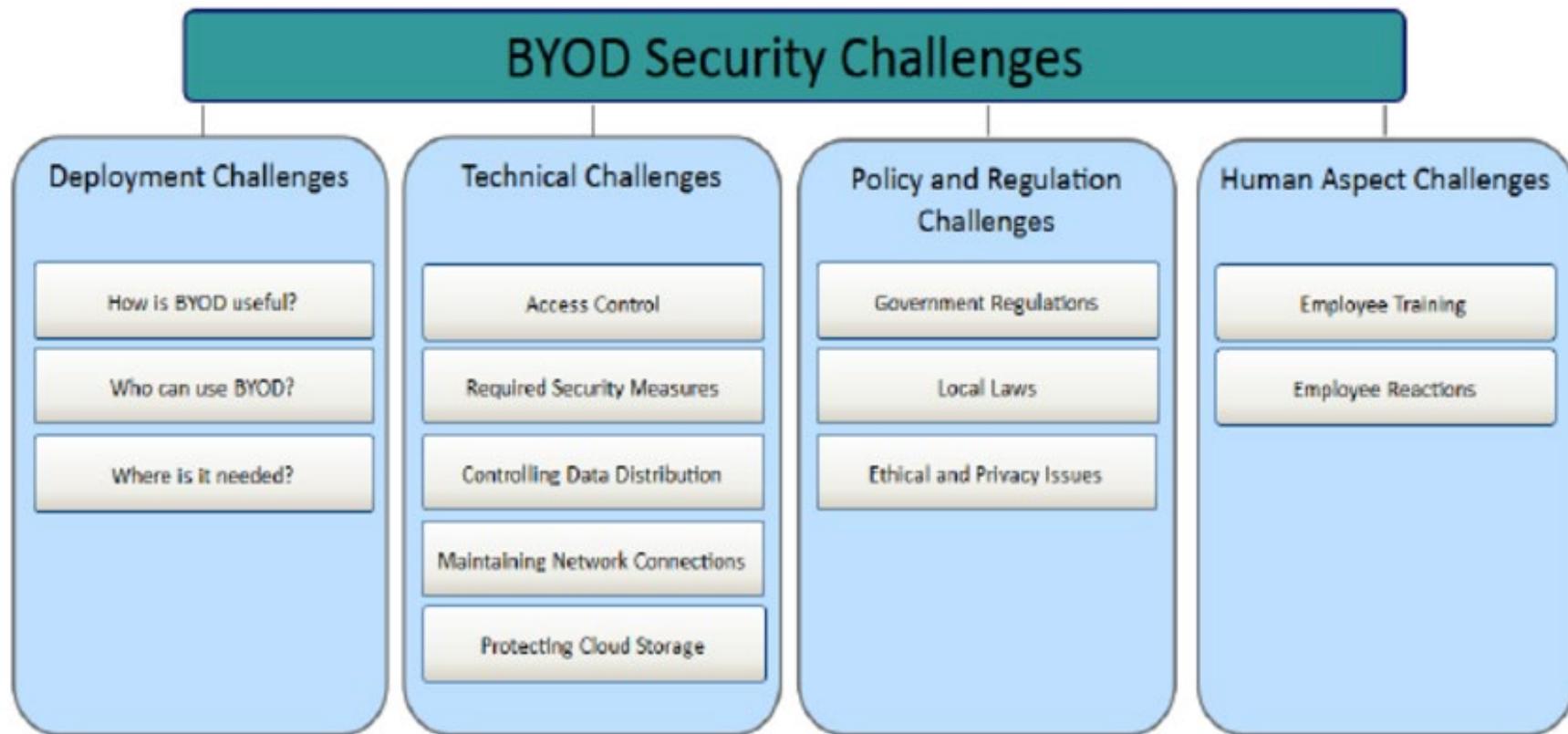
- Assigns wrong time to the client systems and devices
- Requires the internal NTP server to correctly display time



For the systems to synchronize their time, NTP is critical. Most organizations have an internal NTP server configured to synchronize itself with the main NTP servers. Events that get logged in the system have a time stamp. The logs will contain incorrect attack timing. If the time stamp is incorrect, you may not be able to know the actual time if an attack occurs.

To resolve the NTP issues, you should ensure that the systems are correctly synchronized with the internal NTP servers.

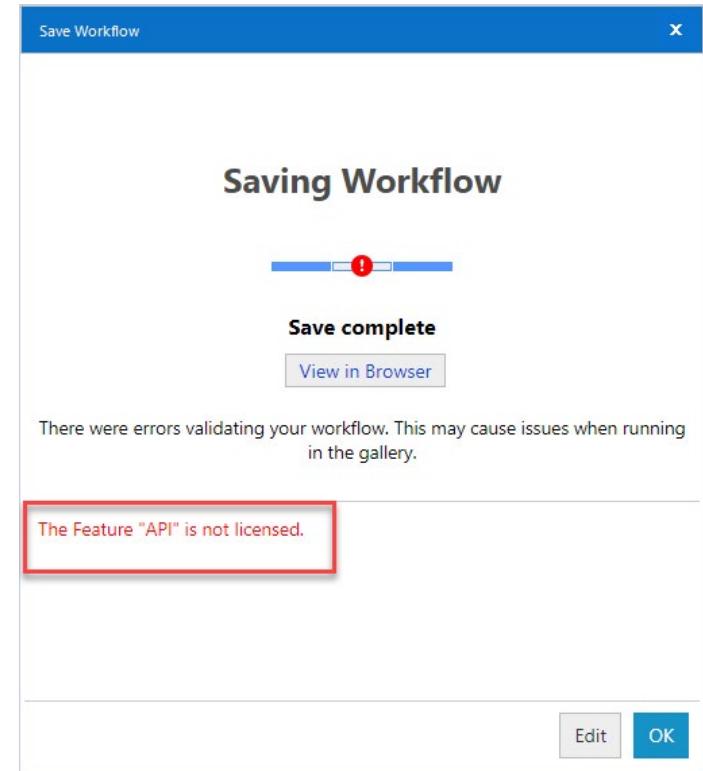
# BYOD Challenges



Bring-your-own-device (BYOD) allows the employees to carry their own devices in an organization. Organizations save much money. For example, rather than an organization spending money on purchasing mobile phones for the employees, they allow them to purchase their own devices and use them for official work. However, with BYOD, you must deal with several issues, as shown on the slide. Each one of them is self-explanatory. One of the main methods to keep strict control on BYOD is to use Mobile Device Management, MDM, which can implement strict security on mobile devices.

# Licensed Feature Issues

- Occurs when a user is using unlicensed application
- Can also occur when a subscription does not cover a specific feature



Several software development organizations allow the users to use their software without any purchase or subscription but with limited features. When you have to use all features within an application, you have to purchase or subscribe to it with a specific fee. For example, Microsoft allows users to use Office 365 for one month free of cost. However, most features, such as saving the file or copy-pasting, are disabled after one month.

If you face any such issue, you should verify if you are using a limited version copy of the software. If yes, then you may have to upgrade.

# Network Performance Issues

- Can be due to
  - Temperature
  - Latency
  - Jitter
  - Wireless channel utilization
  - Bandwidth



[Network Performance Monitoring for Network Troubleshooting | Obkio](#)

The network performance issues can occur due to various reasons:

- Temperature
- Latency
- Jitter
- Wireless channel utilization
- Bandwidth

To resolve any of these issues, you have to monitor the network performance. With continuous monitoring, you will be able to track the issues causing a bottleneck in the network.

# Summary

- Considerations
- Common Issues



That's the end of the lesson.

Here we covered:

- Considerations
- Common Issues

