

कंप्यूटर नेटवर्क टेक्नोलॉजी

नीचे 100 प्रमुख बिंदुओं की सूची है जो “कंप्यूटर नेटवर्क टेक्नोलॉजी” कोर्स या स्व-स्टडी आउटलाइन का विस्तृत क्षेत्र कवर करती है, जिसमें मूलभूत अवधारणाएं, प्रोटोकॉल और व्यावहारिक अनुप्रयोग शामिल हैं।

1. कंप्यूटर नेटवर्क का परिभाषा: एक प्रणाली जिसमें इंटरकनेक्टेड डिवाइस रिसोर्स और डेटा शेयर करते हैं।
2. नेटवर्क के प्राथमिक कार्य: रिसोर्स शेयरिंग, संचार, डेटा ट्रांसमिशन और सहयोग।
3. नेटवर्क का विकास: 1960 और प्रारंभिक 1970 से आज के ग्लोबल इंटरनेट तक।
4. आम नेटवर्क प्रकार: LAN (लोकल एरिया नेटवर्क), MAN (मेट्रोपॉलिटन एरिया नेटवर्क), WAN (वाइड एरिया नेटवर्क)।
5. टोपोलॉजी संरचनाएं: बस, स्टार, रिंग, मेश, और हाइब्रिड।
6. इन्ट्रानेट LAN, एक्स्ट्रानेट WAN, इंटरनेट: स्कोप के अंतर और सामान्य उपयोग मामले।
7. मानक संगठन: IEEE, ISO, IETF—नेटवर्क मानकों और प्रोटोकॉल को परिभाषित और बनाए रखना।
8. OSI रेफरेंस मॉडल: नेटवर्क कार्य को समझने के लिए एक सात-लेयर संकल्पनात्मक फ्रेमवर्क।
9. TCP/IP मॉडल: इंटरनेट को आधारभूत बनाने वाला चार-लेयर (या कभी-कभी पांच-लेयर) व्यावहारिक मॉडल।
10. LAN और WAN की तुलना: समानताएं (लेयर्ड अप्रोच) और अंतर (लेयर की संख्या और संरचना)।
11. भौतिक लेयर का उद्देश्य: भौतिक माध्यम पर कच्चे बिट्स का ट्रांसमिशन से संबंधित।
12. आम ट्रांसमिशन मीडिया: ट्विस्टेड-पेयर केबल, कोएक्सियल केबल, ऑप्टिकल फाइबर, और वायरलेस।
13. बैंडविड्थ Mbps, थ्रूपुट: सिद्धांतिक अधिकतम दर Mbps, वास्तविक डेटा ट्रांसफर दर।
14. सिग्नल एन्कोडिंग: डेटा बिट्स को ट्रांसमिशन के लिए प्रतिनिधित्व करने के लिए विधियां (उदाहरण के लिए, मैनचेस्टर एन्कोडिंग)।
15. मोड्यूलेशन तकनीकें: एएम, एफएम, पीएम का उपयोग एनालॉग-टू-डिजिटल या डिजिटल-टू-एनालॉग परिवर्तनों में।
16. भौतिक लेयर डिवाइस: हब्स, रिपीटर—प्राथमिक रूप से सिग्नल को बिना जांच के दोहराना।
17. डेटा लिंक लेयर का उद्देश्य: फ्रेमिंग, एड्रेसिंग, त्रुटि पता लगाना/सुधार, और फ्लो कंट्रोल का प्रबंधन।
18. फ्रेमिंग: डेटा लिंक लेयर हेडर और ट्रेलर में पैकेट को कैप्स्यूलेट करना।
19. MAC (मीडिया एक्सेस कंट्रोल) एड्रेस: नेटवर्क इंटरफेस कार्ड के लिए एक अनोखी हार्डवेयर पहचान।
20. त्रुटि पता लगाने की विधियां: पैरिटी चेक, CRC (साइक्लिक रेडंडेंसी चेक), चेकसम।
21. ईथर्नेट बेसिक्स: सबसे आम LAN प्रौद्योगिकी; स्रोत/गंतव्य MAC का उपयोग करते हुए एक फ्रेम संरचना का उपयोग करती है।
22. ईथर्नेट फ्रेम फॉर्मेट: प्रीएम्बल, गंतव्य MAC, स्रोत MAC, प्रकार/लंबाई, पेलोड, ट्रेलर।
23. स्विचिंग: MAC एड्रेस टेबल का उपयोग करके एक MAC में फ्रेम फॉरवर्ड करना।
24. स्विच में सीखने की प्रक्रिया: डिवाइस संचार करते समय MAC एड्रेसों की एक टेबल बनाना।
25. VLAN (वर्चुअल LAN): एक भौतिक LAN को कई वर्चुअल नेटवर्कों में तार्किक रूप से विभाजित करना।

26. नेटवर्क लेयर का उद्देश्य: रूटिंग, तार्किक एड्रेसिंग (IP), और पथ निर्धारण।
27. IPv4 एड्रेस फॉर्मेट: 32-बिट एड्रेस, आमतौर पर डॉटेड-डेसीमल नोटेशन में प्रतिनिधित्व किया जाता है।
28. IPv4 क्लासेज (अवैध): क्लास A, B, C, D, E (इतिहासिक संदर्भ, IANA द्वारा प्रतिस्थापित)।
29. IPv6 (क्लासलेस इंटर-डोमेन रूटिंग): अधिक लचीला IPv4 एड्रेस आवंटन के लिए आधुनिक दृष्टिकोण।
30. IPv4 vs. IPv6: मुख्य अंतर (128-बिट एड्रेसिंग, विस्तृत हेडर फॉर्मेट, स्व-आयोजन)।
31. सबनेटिंग: बड़े नेटवर्क को छोटे सबनेटवर्क में विभाजित करना, प्रभावी एड्रेस उपयोग के लिए।
32. VLSM (नेटवर्क एड्रेस ट्रांसलेशन): निजी IPv4 एड्रेस को एक सार्वजनिक IPv4 पर मैप करना, IPv4 एड्रेसों को बचाना।
33. NAT (एड्रेस रिज़ॉल्यूशन प्रोटोकॉल): एक IPv4 में IPv4 एड्रेस को IPv6 में परिवर्तित करना।
34. ICMP (इंटरनेट कंट्रोल मैसेज प्रोटोकॉल): डायग्नोस्टिक टूल—पिंग, ट्रेसरूट द्वारा उपयोग किया जाता है।
35. रूटिंग vs. स्विचिंग: रूटिंग IPv4-स्तर (लेयर 3) के लिए है, जबकि स्विचिंग IPv2-स्तर (लेयर 2) के लिए है।
36. स्टैटिक रूटिंग: राउटर के रूटिंग टेबल में रूट्स को हाथ से कॉन्फ़िगर करना।
37. डायनामिक रूटिंग प्रोटोकॉल: RIPv2 (रूटिंग इंफ़ॉर्मेशन प्रोटोकॉल), OSPF (ओपन शॉर्टेस्ट पाथ फ़र्स्ट), BGP (बॉर्डर गेटवे प्रोटोकॉल)।
38. राउटर बेसिक्स: IPv4 एड्रेसों के आधार पर एक पैकेट के लिए अगले नेटवर्क हॉप को निर्धारित करना।
39. ट्रांसपोर्ट लेयर का उद्देश्य: एंड-टू-एंड डेटा डिलीवरी, विश्वसनीयता, और फ्लो कंट्रोल।
40. TCP (ट्रांसमिशन कंट्रोल प्रोटोकॉल): विश्वसनीय डेटा ट्रांसफर प्रदान करने वाला कनेक्शन-ओरिएंटेड प्रोटोकॉल।
41. TCP सेगमेंट संरचना: स्रोत पोर्ट, गंतव्य पोर्ट, सीक्वेंस नंबर, एक्नॉलेजमेंट नंबर, आदि।
42. TCP तीन-वे हैंडशेक: कनेक्शन सेटअप के लिए SYN, SYN-ACK, ACK प्रक्रिया।
43. TCP चार-वे टीयरडाउन: कनेक्शन को बंद करने के लिए FIN, FIN-ACK, RST अनुक्रम।
44. TCP फ्लो कंट्रोल: डेटा ट्रांसफर दरों को प्रबंधित करने के लिए स्लाइडिंग विंडो जैसे यंत्र।
45. TCP कांजेशन कंट्रोल: एल्गोरिथम (स्लो स्टार्ट, कांजेशन एवॉइडेंस, फास्ट रिकवरी, फास्ट रिट्रांसमिट)।
46. UDP (यूजर डाटाग्राम प्रोटोकॉल): कनेक्शनलेस, न्यूनतम ओवरहेड, डिलीवरी की गारंटी नहीं।
47. UDP सेगमेंट संरचना: स्रोत पोर्ट, गंतव्य पोर्ट, लंबाई, चेकसम, डेटा।
48. पोर्ट नंबर: सेवा के लिए पहचानकर्ता (उदाहरण के लिए, 80 के लिए HTTP, 443 के लिए HTTPS, 53 के लिए DNS)।
49. सॉकेट: एक एंडपॉइंट को पहचानने के लिए IPv4 और पोर्ट का संयोजन।
50. एप्लिकेशन लेयर का उद्देश्य: उपयोगकर्ता एप्लिकेशन को नेटवर्क सेवाएं प्रदान करता है।
51. HTTP (हाइपरटेक्स्ट ट्रांसफर प्रोटोकॉल): वेब पर डेटा संचार का आधार।
52. HTTP विधियाँ: GET, POST, PUT, DELETE, HEAD, आदि।
53. HTTPS: HTTP/TCP का उपयोग करके एनक्रिप्टेड HTTP के लिए सुरक्षित वेब संचार।

54. □□□ (डोमेन नेम सिस्टम): डोमेन नाम (उदाहरण के लिए, □□□□□□□.□□□) को □□ एड्रेस में मैप करता है।
55. □□□ रिज़ॉल्यूशन प्रक्रिया: रिकर्सिव और इटरेटिव क्वेरी, रूट सर्वर, □□□ सर्वर, अधिकारिक सर्वर।
56. □□□ (फाइल ट्रांसफर प्रोटोकॉल): □□□ (पोर्ट 20/21) पर फाइल ट्रांसफर्स के लिए पुराना प्रोटोकॉल।
57. ईमेल प्रोटोकॉल: □□□□ (सैंड), □□□3 और □□□□ (रिट्रीव)।
58. □□□□ (डायनामिक होस्ट कन्फिगरेशन प्रोटोकॉल): डिवाइसों को स्वचालित रूप से □□ एड्रेस आवंटित करता है।
59. टेलनेट □□. □□□: रिमोट एक्सेस प्रोटोकॉल—□□□ एनक्रिप्टेड है, टेलनेट नहीं है।
60. क्लाइंट-सर्वर मॉडल: एक आम आर्किटेक्चर जहां एक क्लाइंट एक सर्वर से सेवाएं अनुरोध करता है।
61. □2□ (पीयर-टू-पीयर) मॉडल: प्रत्येक नोड दोनों सेवाएं अनुरोध कर सकता है और प्रदान कर सकता है।
62. वेब प्रौद्योगिकी: □□□□, □□□□, कुकीज, सेशन, बेसिक वेब एप्लिकेशन संरचना।
63. नेटवर्क सुरक्षा सिद्धांत: गोपनीयता, पूर्णता, उपलब्धता (□□□ त्रिकोण)।
64. आम सुरक्षा खतरे: मलवेयर (वायरस, वर्म, ट्रॉजन), □□□□ हमले, फिशिंग, □□□ इंजेक्शन।
65. फायरवॉल: नियमों के आधार पर ट्रैफिक को फिल्टर करता है, नेटवर्क सीमाओं पर रखा जाता है।
66. □□□/□□□ (इंट्रूजन डिटेक्शन/प्रिवेंशन सिस्टम): संदिग्ध गतिविधियों के लिए ट्रैफिक को निगरानी करता है।
67. □□□ (वर्चुअल प्राइवेट नेटवर्क): सार्वजनिक नेटवर्क पर एनक्रिप्टेड टनल, दूरस्थ कनेक्शन को सुरक्षित करता है।
68. □□□/□□□ (ट्रांसपोर्ट लेयर सिक्वोरिटी / सिक्वोर सॉकेट्स लेयर): सुरक्षित डेटा ट्रांसफर के लिए एनक्रिप्शन।
69. क्रिप्टोग्राफी बेसिक्स: सममित्रिक □□. असममित्रिक एनक्रिप्शन, की एक्सचेंज, डिजिटल हस्ताक्षर।
70. डिजिटल सर्टिफिकेट: □□□ (सर्टिफिकेट ऑथोरिटी) द्वारा प्रदान किए जाते हैं, पहचान को सत्यापित करने और □□□□□ को सक्षम बनाने के लिए।
71. नेटवर्क सुरक्षा नीति: सुरक्षित नेटवर्क उपयोग, एक्सेस कंट्रोल और ऑडिट के लिए दिशा-निर्देश।
72. □□□ (डेमिलिटराइज्ड ज़ोन): एक सबनेट जो बाहरी-फेसिंग सेवाओं को सार्वजनिक रूप से प्रदर्शित करता है।
73. □□□□ सुरक्षा: वायरलेस नेटवर्क (□□-□□) को □□□2, □□□3, आदि द्वारा सुरक्षित किया जाता है।
74. भौतिक सुरक्षा: नेटवर्क इंफ्रास्ट्रक्चर (सर्वर, केबल, राउटर) को सुरक्षित रूप से रखा जाता है।
75. सामाजिक इंजीनियरिंग: तकनीकी न होने वाले प्रवेश तकनीक—फिशिंग, प्रेटेक्स्टिंग, बैटिंग।
76. □□□ लेयर हमले: प्रत्येक लेयर पर अलग-अलग खतरे/रक्षा (उदाहरण के लिए, □□□ स्पूफिंग डेटा लिंक लेयर पर)।
77. नेटवर्क प्रशासन टूल: पिंग, ट्रेसरूट, नेटस्टैट, न्सलुक, डिग।
78. पैकेट स्निफर: □□□□□□□□ या □□□□□□□□ जैसे टूल पैकेट स्तर पर ट्रैफिक का विश्लेषण करने के लिए।
79. नेटवर्क प्रबंधन प्रोटोकॉल: □□□□ (सिम्पल नेटवर्क मैनेजमेंट प्रोटोकॉल)।
80. लॉगिंग और मॉनिटरिंग: सिस्लॉग, इवेंट लॉग, □□□□ सॉल्यूशन के लिए वास्तविक समय में पता लगाना।
81. बेसिक □□□ सेटअप: □□ रेंज, सबनेट मास्क, गेटवे, □□□ सर्वर निर्धारित करना।

82. केबल प्रकार: 0005, 00050, 0006, फाइबर ऑप्टिक, प्रत्येक का आमतौर पर उपयोग।
83. संरचित केबलिंग: पेशेवर बड़े पैमाने पर नेटवर्क इंस्टॉलेशन के लिए मानक।
84. स्विच कॉन्फिगरेशन: 00000, ट्रंक पोर्ट, और स्पैनिंग ट्री प्रोटोकॉल बनाना।
85. राउटर कॉन्फिगरेशन: रूट्स (स्टैटिक/डायनामिक), 000, 000 (एक्सेस कंट्रोल लिस्ट) सेटअप करना।
86. बेसिक फायरवॉल नियम: सभी इनबाउंड को अस्वीकार करें सिवाय आवश्यक, सभी आउटबाउंड को अनुमति दें या आवश्यकता के अनुसार सीमित करें।
87. नेटवर्क एड्रेसिंग प्लान: विभाग या सबनेट के आधार पर 00 एड्रेस को प्रभावी रूप से आवंटित करना।
88. रेडडेंसी और फेलओवर: बैकअप लिंक, लोड बैलेंसिंग, या 0000/0000 का उपयोग उच्च उपलब्धता के लिए।
89. 000 (क्वालिटी ऑफ सर्विस): कुछ ट्रैफिक (उदाहरण के लिए, 0000) को प्राथमिकता देना, प्रदर्शन सुनिश्चित करने के लिए।
90. क्लाउड नेटवर्किंग बेसिक्स: क्लाउड पर्यावरण में वर्चुअल नेटवर्क, सुरक्षा समूह, लोड बैलेंसर।
91. 000 (सॉफ्टवेयर-डिफाईंड नेटवर्किंग): केंद्रित प्रबंधन के लिए नियंत्रण प्लेन को डेटा प्लेन से अलग करना।
92. वर्चुअलाइजेशन: हाइपरवाइजर (000000, 00000-0, 000) का उपयोग करके वर्चुअल सर्वर/नेटवर्क बनाना।
93. कंटेनर और माइक्रोसर्विसेज: डॉकर नेटवर्क, क्यूबर्नेट्स नेटवर्किंग अवधारणाएं।
94. 0006 डिप्लॉयमेंट: ड्यूल स्टैक (0004/0006), 0006 स्व-आयोजन (00000), 0006 टनल।
95. 000 लोड बैलेंसिंग: 000 राउंड रॉबिन के माध्यम से ट्रैफिक को कई सर्वरों पर वितरित करना।
96. एज कंप्यूटिंग: 000 और वास्तविक समय सेवाओं के लिए लेटेंसी को कम करने के लिए नेटवर्क के एज पर प्रोसेसिंग।
97. 50 और वायरलेस विकास: उच्च डेटा दर, कम लेटेंसी, 000 और मोबाइल ब्रॉडबैंड में उपयोग।
98. नेटवर्क ट्रबलशूटिंग चरण: समस्या को पहचानें, अलग करें, हाइपोथेसिस परीक्षण करें, ठीक करें, सत्यापित करें।
99. दस्तावेजीकरण: नेटवर्क डायग्राम और डिवाइस कॉन्फिगरेशन को सही रखने की महत्वता।
100. लगातार सीखना: नेटवर्किंग हमेशा विकसित होती रहती है, नए प्रोटोकॉल और बेस्ट प्रैक्टिस का लगातार अध्ययन करने की आवश्यकता होती है।

ये 100 बिंदु कंप्यूटर नेटवर्क में आवश्यक विषयों को सारांशित करते हैं, जिसमें मूलभूत सिद्धांत, प्रोटोकॉल, हार्डवेयर, एड्रेसिंग, सुरक्षा और आधुनिक प्रवृत्तियां शामिल हैं। वे आपके परीक्षा के लिए या कंप्यूटर नेटवर्किंग के व्यावहारिक समझ के लिए अध्ययन और समीक्षा को मार्गदर्शित करने में मदद कर सकते हैं।