یونٹ 6: کمپیوٹر نیٹ ورکس

سوال نمبر 1: میک ایڈریس کیا ہے؟

جواب: میک ایڈریس (MAC Address) کا مطلب "Media Access Control Address" ہے۔ یہ ایک منفرد ہارڈ ویئر شناختی نمبر ہے جو نیٹ ورک سے منسلک ہر ڈیوائس (جیسے کمپیوٹر، اسمارٹ فون) کو اس کے مینوفیکچرر کی طرف سے دیا جاتا ہے۔ سوئچز اس ایڈریس کا استعمال کرتے ہوئے ڈیٹا پیکٹس کو درست ڈیوائس تک پہنچاتے ہیں۔

سوال نمبر 2: کمپیوٹر نیٹ ورک کے بنیادی اجزاء کون سے ہیں؟

جواب: کمپیوٹر نیٹ ورک کے بنیادی اجزاء وہ عناصر ہیں جو مل کر ایک نیٹ ورک بناتے ہیں اور ڈیٹا کی ترسیل کو ممکن بناتے ہیں۔ ان میں نوڈز (ڈیوائسز)، لنکس (رابطے)، سوئچز، اور راؤٹرز شامل ہیں۔

سوال نمبر 3: کمپیوٹر نیٹ ورکس کے بنیادی اجزاء کی فہرست بنائیں۔

جواب: کمپیوٹر نیٹ ورک کے بنیادی اجزاء درج ذیل ہیں:

- **نوڈز (Nodes):** نیٹ ورک سے منسلک ڈیوائسز جیسے کمپیوٹرز، اسمارٹ فونز، اور پرنٹرز۔
- **لنکس (Links):** نوڈز کے درمیان رابطے، جو وائرڈ (جیسے ایتھرنیٹ کیبل) یا وائرلیس (جیسے وائی فائی) ہو سکتے ہیں۔
- **سوئچز (Switches):** وہ ڈیوائسز جو ایک ہی نیٹ ورک کے اندر متعدد نوڈز کو جوڑتی ہیں اور ڈیٹا کو آگے بھیجتی ہیں۔
- **راؤٹرز (Routers):** وہ ڈیوائسز جو مختلف نیٹ ورکس کو آپس میں جوڑتی ہیں اور ڈیٹا پیکٹس کو ان کے درمیان ہدایت دیتی ہیں۔

سوال نمبر 4: کمپیوٹر نیٹ ورک وسائل کو کیسے شیئر کرتے ہیں؟ مثال بھی لکھیں۔

جواب: کمپیوٹر نیٹ ورکس ڈیوائسز کو وسائل (resources) کا اشتراک کرنے کی اجازت دیتے ہیں، جس سے اخراجات کم ہوتے ہیں اور کارکردگی بہتر ہوتی ہے۔ **مثال:** ایک دفتر کے نیٹ ورک میں، متعدد کمپیوٹرز ایک ہی پرنٹر کا اشتراک کر سکتے ہیں، جس سے ہر کمپیوٹر کے لیے الگ پرنٹر خریدنے کی ضرورت ختم ہو جاتی ہے۔

سوال نمبر 5: کمپیوٹر نیٹ ورکس کمیونیکیشن میں کس طرح مدد کرتے ہیں؟

جواب: کمپیوٹر نیٹ ورکس ای میلز، فوری پیغام رسانی (instant messaging)، اور ویڈیو کانفرنسنگ کے ذریعے ڈیٹا کی منتقلی کو آسان بنا کر مؤثر مواصلات کو ممکن بناتے ہیں۔

سوال نمبر 6: ویڈیو کانفرنسنگ کیا ہوتی ہے؟

جواب: ویڈیو کانفرنسنگ ایک ایسی ٹیکنالوجی ہے جو کمپیوٹر نیٹ ورکس کا استعمال کرتے ہوئے مختلف مقامات پر موجود لوگوں کو آڈیو اور ویڈیو کے ذریعے حقیقی وقت میں بات چیت کرنے کی اجازت دیتی ہے۔ زوم (Zoom) اور مائیکروسافٹ ٹیمز (Microsoft Teams) اس کی عام مثالیں ہیں۔

سوال نمبر 7: کمپیوٹر نیٹ ورک کنیکٹیویٹی اور تعاون کو کیسے فعال کر سکتا ہے؟

جواب: کمپیوٹر نیٹ ورکس آلات کو آپس میں جوڑ کر ریموٹ رسائی (remote access) اور تعاون (collaboration) کی اجازت دیتے ہیں۔ اس سے ٹیمیں ایک ساتھ مل کر کام کر سکتی ہیں، چاہے وہ مختلف جگہوں پر موجود ہوں۔ اس سے پیداواری صلاحیت اور لچک میں اضافہ ہوتا ہے۔

سوال نمبر 8: گوگل ڈرائیو کیا ہے؟

جواب: گوگل ڈرائیو (Google Drive) ایک کلاؤڈ پر مبنی سروس ہے جو صارفین کو فائلوں کو آن لائن ذخیرہ کرنے اور ان کا اشتراک کرنے کی اجازت دیتی ہے۔ یہ ایک کمپیوٹر نیٹ ورک کی مثال ہے جو تعاون کو ممکن بناتی ہے، کیونکہ ایک ٹیم گوگل ڈرائیو کا استعمال کرتے ہوئے حقیقی وقت میں ایک ہی دستاویز پر کام کر سکتی ہے۔

سوال نمبر 9: کمپیوٹر نیٹ ورک کیا ہوتا ہے؟

جواب: کمپیوٹر نیٹ ورک آپس میں جڑے ہوئے آلات اور کمپیوٹرز کا ایک نظام ہے جو ڈیٹا کا تبادلہ کر سکتے ہیں اور ایک ساتھ کام کر سکتے ہیں۔ یہ چھوٹے، مقامی ایریا نیٹ ورکس (LANs) سے لے کر بڑے، وسیع ایریا نیٹ ورکس (WANs) جیسے انٹرنیٹ تک ہو سکتے ہیں۔

سوال نمبر10: کمپیوٹر نیٹ ورک کی مثال دیں۔

جواب: کمپیوٹر نیٹ ورک کی سب سے بڑی اور عام مثال **انٹرنیٹ** ہے، جو دنیا بھر کے اربوں کمپیوٹرز اور نیٹ ورکس کو آپس میں جوڑتا ہے۔

سوال نمبر11: ہم کمپیوٹر نیٹ ورک کیوں استعمال کرتے ہیں؟

جواب: ہم کمپیوٹر نیٹ ورک کا استعمال وسائل کا اشتراک کرنے (جیسے پرنٹرز)، ڈیٹا کا تبادلہ کرنے (جیسے ای میل بھیجنا)، اور تعاون کو بہتر بنانے (جیسے مشترکہ دستاویزات پر کام کرنا) کے لیے کرتے ہیں۔

سوال نمبر12: نیٹ ورکنگ ڈیوائسز کیا ہوتی ہیں؟

جواب: نیٹ ورکنگ ڈیوائسز وہ ہارڈ ویئر آلات ہیں جو نیٹ ورک ٹریفک کو منظم کرنے اور ہدایت دینے کے ذمہ دار ہیں۔ ان میں ہب، سوئچ، راؤٹر، اور ایکسیس پوائنٹ شامل ہیں۔

سوال نمبر13: چار نیٹ ورکنگ ڈیوائسوں کے نام لکھیں۔

جواب: چار نیٹ ورکنگ ڈیوائسز یہ ہیں:

1. سوئچ (Switch)
2. راؤٹر (Router)
3. ایکسیس پوائنٹ (Access Point)
4. ہب (Hub)

سوال نمبر14: نیٹ ورک میں سوئچ کا کیا کردار ہوتا ہے؟

جواب: نیٹ ورک میں سوئچ کا کردار متعدد نیٹ ورک ڈیوائسز (جیسے کمپیوٹرز، پرنٹرز) کو ایک ہی نیٹ ورک کے اندر جوڑنا ہے تاکہ وہ ایک دوسرے کے ساتھ مؤثر طریقے سے بات چیت کر سکیں۔

سوال نمبر15: سوئچ کس طرح کام کرتا ہے؟

جواب: سوئچ OSI ماڈل کی ڈیٹا لنک لیئر (لیئر 2) پر کام کرتا ہے۔ یہ ڈیٹا پیکٹ میں موجود منزل کے میک ایڈریس (MAC Address) کو پڑھتا ہے اور پیکٹ کو صرف اسی ڈیوائس کو بھیجتا ہے جس کا وہ ایڈریس ہوتا ہے، بجائے اس کے کہ وہ اسے تمام ڈیوائسز کو بھیجے۔

سوال نمبر16: ہب اور سوئچ میں کیا فرق ہے؟

جواب: ہب (Hub) اور سوئچ (Switch) میں بنیادی فرق یہ ہے کہ ہب جب کوئی ڈیٹا پیکٹ وصول کرتا ہے تو اسے اپنے ساتھ منسلک تمام ڈیوائسز کو بھیج دیتا ہے (براڈکاسٹ کرتا ہے)۔ اس کے برعکس، سوئچ زیادہ ذہین ہوتا ہے اور ڈیٹا پیکٹ کو صرف اس کی مخصوص منزل والی ڈیوائس کو بھیجتا ہے، جس سے نیٹ ورک کی کارکردگی بہتر ہوتی ہے۔

سوال نمبر17: راؤٹر کس طرح کام کرتا ہے؟

جواب: راؤٹر مختلف نیٹ ورکس کو آپس میں جوڑتا ہے اور ڈیٹا پیکٹس کو ان کے درمیان ہدایت دیتا ہے۔ یہ ہر ڈیٹا پیکٹ کے لیے بہترین راستہ تلاش کرنے کے لیے ایک "راؤٹنگ ٹیبل" کا استعمال کرتا ہے تاکہ ڈیٹا مؤثر طریقے سے اپنی منزل تک پہنچ سکے۔

سوال نمبر18 SIM: کارڈ کیا ہوتا ہے؟

جواب: سم (SIM) کا مطلب "Subscriber Identity Module" ہے۔ یہ ایک چھوٹا کارڈ ہے جو موبائل ڈیوائس میں ڈالا جاتا ہے۔ اس میں سبسکرائبر کی شناخت اور تصدیق کے لیے منفرد معلومات ہوتی ہیں، جس سے ڈیوائس موبائل نیٹ ورک سے منسلک ہو کر کالز کرنے، پیغامات بھیجنے اور انٹرنیٹ تک رسائی حاصل کر سکتی ہے۔

سوال نمبر19: ایکسس پوائنٹ کے بارے میں آپ کیا جانتے ہیں؟

جواب : ایکسیس پوائنٹ (Access Point – AP) ایک نیٹ ورکنگ ڈیوائس ہے جو وائرلیس ڈیوائسز کو ایک وائرڈ نیٹ ورک سے منسلک ہونے کی سہولت فراہم کرتی ہے۔ یہ آپ کے کمپیوٹرز، اسمارٹ فونز اور انٹرنیٹ کے درمیان ایک پل کا کام کرتا ہے اور ریڈیو لہروں کا استعمال کرتے ہوئے ڈیٹا منتقل کرتا ہے۔

سوال نمبر20: ٹپالوجی کی تعریف کریں اور عام نیٹ ورک ٹپالوجی کی فہرست بنائیں۔

جواب : ٹپالوجی : نیٹ ورک ٹپالوجی سے مراد کمپیوٹر نیٹ ورک میں مختلف آلات (نوڈز) کی ترتیب یا ساخت ہے۔ **عام ٹپالوجیز:**

- بس ٹپالوجی (Bus Topology)
- اسٹار ٹپالوجی (Star Topology)
- رنگ ٹپالوجی (Ring Topology)
- میش ٹپالوجی (Mesh Topology)

سوال نمبر21: بس ٹپالوجی کیا ہے؟

جواب : بس ٹپالوجی میں، تمام ڈیوائسز ایک ہی مرکزی مواصلاتی لائن کا اشتراک کرتی ہیں جسے "بس" کہا جاتا ہے۔ ہر ڈیوائس اس مرکزی کیبل سے منسلک ہوتی ہے۔

سوال نمبر22: اسٹار ٹپالوجی کیا ہے؟

جواب : اسٹار ٹپالوجی میں، ہر نوڈ ایک مرکزی سوئچ یا ہب کے ذریعے دوسروں کے ساتھ بات چیت کرتا ہے۔ تمام ڈیٹا مرکزی ڈیوائس سے گزرتا ہے۔

سوال نمبر23: اسٹار ٹپالوجی کے بڑے نقصانات کیا ہیں؟

جواب : اسٹار ٹپالوجی کا سب سے بڑا نقصان یہ ہے کہ اگر مرکزی ہب یا سوئچ ناکام ہو جائے تو پورا نیٹ ورک بند ہو جاتا ہے۔

سوال نمبر24: رنگ ٹپالوجی کیا ہے؟

جواب : رنگ ٹپالوجی میں، ہر ڈیوائس ایک سرکلر راستے میں دوسری ڈیوائسز سے منسلک ہوتی ہے۔ ڈیٹا ایک ہی سمت میں سفر کرتا ہے اور ہر ڈیوائس سے گزرتا ہے۔

سوال نمبر25: میش ٹپالوجی کیا ہے؟

جواب : میش ٹپالوجی میں، ہر ڈیوائس ہر دوسری ڈیوائس سے براہ راست منسلک ہوتی ہے۔ یہ اعلیٰ درجے کی فالتو پن (redundancy) اور قابل اعتمادی فراہم کرتی ہے۔

سوال نمبر26: ڈیٹا ٹرانسمیشن کی تعریف کریں اور اس کی اقسام لکھیں۔

جواب : ڈیٹا ٹرانسمیشن : اس سے مراد آلات کے درمیان ڈیٹا کی ترسیل کا طریقہ ہے۔ **اقسام (موڈز):**

1. سمپلیکس (Simplex)
2. ہاف-ڈوپلیکس (Half-Duplex)
3. فل-ڈوپلیکس (Full-Duplex)

سوال نمبر27: سمپلیکس موڈ کیا ہوتا ہے؟ج

واب : سمپلیکس موڈ میں، ڈیٹا کی ترسیل یک طرفہ ہوتی ہے، یعنی یہ صرف ایک ہی سمت میں بہتی ہے۔ ایک ڈیوائس یا تو ڈیٹا بھیج سکتی ہے یا وصول کر سکتی ہے، دونوں کام ایک ساتھ نہیں کر سکتی۔ مثال: کی بورڈ سے کمپیوٹر تک ڈیٹا کی منتقلی۔

سوال نمبر28: ہاف ڈوپلیکس موڈ کیا ہے؟

جواب : ہاف-ڈوپلیکس موڈ میں، ڈیٹا کی ترسیل دونوں سمتوں میں ہو سکتی ہے، لیکن بیک وقت نہیں۔ ایک ڈیوائس کو بھیجنے سے پہلے دوسری ڈیوائس کے ٹرانسمیشن ختم کرنے کا انتظار کرنا پڑتا ہے۔ مثال: واکی ٹاکی۔

سوال نمبر29: فل ڈوپلیکس موڈ کیا ہے؟

جواب : فل-ڈوپلیکس موڈ دونوں سمتوں میں بیک وقت ڈیٹا کی ترسیل کی اجازت دیتا ہے۔ دونوں ڈیوائسز ایک ہی وقت میں ڈیٹا بھیج اور وصول کر سکتی ہیں۔ مثال: ٹیلی فون پر گفتگو۔

سوال نمبر30: ہاف اور فل ڈوپلیکس ٹرانسمیشن موڈ میں فرق بیان کریں۔

جواب: ہاف-ڈوپلیکس میں ڈیٹا دونوں طرف جاسکتا ہے لیکن ایک وقت میں صرف ایک طرف۔ فل-ڈوپلیکس میں ڈیٹا بیک وقت دونوں طرف جااور آسکتا ہے۔

سوال نمبر31 OSI: ماڈل کی سات لیئرز کے نام لکھیں۔

جواب:

1. فزیکل لیئر (Physical Layer)
2. ڈیٹالنک لیئر (Data Link Layer)
3. نیٹ ورک لیئر (Network Layer)
4. ٹرانسپورٹ لیئر (Transport Layer)
5. سیشن لیئر (Session Layer)
6. پریزنٹیشن لیئر (Presentation Layer)
7. ایپلیکیشن لیئر (Application Layer)

سوال نمبر32 OSI: ماڈل میں فزیکل لیئر کا کیا کردار ہوتا ہے؟

جواب: فزیکل لیئر آلات کے درمیان حقیقی طبعی رابطے کی ذمہ دار ہے۔ یہ خام ڈیٹا بٹس کو ایک طبعی میڈیم (جیسے کیبل) کے ذریعے بھیجنے پر توجہ مرکوز کرتی ہے۔

سوال نمبر33 OSI: ماڈل میں ڈیٹالنک لیئر کا کیا کردار ہوتا ہے؟

جواب: ڈیٹالنک لیئر غلطی کی نشاندہی اور اصلاح کے ساتھ ساتھ نوڈ-سے-نوڈ ڈیٹا کی منتقلی کو سنبھالتی ہے۔ یہ یقینی بناتی ہے کہ ڈیٹا فزیکل لیئر سے بغیر کسی غلطی کے منتقل ہو۔

سوال نمبر34 OSI: ماڈل میں ٹرانسپورٹ لیئر کا کیا کردار ہوتا ہے؟

جواب: ٹرانسپورٹ لیئر اس بات کو یقینی بناتی ہے کہ ڈیٹا ایک سورس سسٹم پر چلنے والے پراسیس سے منزل کے سسٹم پر چلنے والے پراسیس تک قابل اعتماد طریقے سے منتقل ہو۔ یہ ڈیٹا کے بہاؤ کو کنٹرول کرتی ہے اور غلطی کی جانچ کرتی ہے۔

سوال نمبر35 OSI: ماڈل میں سیشن لیئر کا کیا کردار ہوتا ہے؟

جواب: سیشن لیئر ایپلی کیشنز کے درمیان سیشنز (رابطوں) کا انتظام کرتی ہے۔ یہ آلات کے درمیان رابطے قائم کرتی ہے، انہیں برقرار رکھتی ہے، اور ختم کرتی ہے۔

سوال نمبر36 OSI: ماڈل میں پریزنٹیشن لیئر کا کیا کردار ہوتا ہے؟ جواب: پریزنٹیشن لیئر ایپلی کیشن لیئر اور نیٹ ورک کے درمیان ڈیٹا کا ترجمہ کرتی ہے۔ یہ ڈیٹا کو فارمیٹ اور انکرپٹ کرتی ہے تاکہ وصول کرنے والا سسٹم اسے پڑھ سکے۔

سوال نمبر37 OSI: ماڈل میں ایپلی کیشن لیئر کا کیا کردار ہوتا ہے؟

جواب: ایپلی کیشن لیئر صارف کے سب سے قریب ہوتی ہے۔ یہ براہ راست ایپلی کیشنز کو نیٹ ورک خدمات فراہم کرتی ہے، جیسے ای میل، ویب براؤزنگ، اور فائل ٹرانسفر۔

سوال نمبر38: آئی پی کا کیا استعمال ہے؟

جواب: آئی پی (انٹرنیٹ پروٹوکول) کا استعمال نیٹ ورک پر موجود آلات کو ایک منفرد ایڈریس تفویض کرنے اور ڈیٹا پیکٹس کو ان کے پتے اور روٹنگ کے لیے کیا جاتا ہے۔

سوال نمبر39 IPv4: کیا ہوتا ہے؟

جواب IPv4: (انٹرنیٹ پروٹوکول ورژن 4) انٹرنیٹ پروٹوکول کا چوتھا ورژن ہے۔ یہ 32-بٹ ایڈریس اسکیم کا استعمال کرتا ہے، جس سے تقریباً 4.3 ارب منفرد ایڈریسز ممکن ہیں۔

سوال نمبر40 IPv6: کیا ہے؟

جواب IPv6 :(انٹرنیٹ پروٹوکول ورژن6)انٹرنیٹ پروٹوکول کا جدید ترین ورژن ہے جسے IPv4 کی جگہ لینے کے لیے ڈیزائن کیا گیا ہے۔ یہ 128-بٹ ایڈریس اسکیم کا استعمال کرتا ہے، جس سے تقریباً محدود تعداد میں منفرد ایڈریسز ممکن ہیں۔

سوال نمبر41 IPv6 :کی کیوں ضرورت تھی؟

جواب IPv6 :کی ضرورت اس لیے پیش آئی کیونکہ انٹرنیٹ اور منسلک آلات کی تیزی سے ترقی کی وجہ سے IPv4 ایڈریسز ختم ہو رہے تھے۔ IPv6 ایڈریسز کی ایک بہت بڑی تعداد فراہم کرتا ہے۔

سوال نمبر42 IPV4 :اور IPv6 میں فرق بیان کریں۔

جواب:

خصوصیت	IPv6	IPv4
ایڈریس سائز	128-بٹ	32-بٹ
ایڈریس کی تعداد	340~انڈیسیلین	4.3~ارب
فارمیٹ	ہیکساڈیسیمل(2001:0db8::8a2e)	ڈاٹڈڈیسیمل(192.168.1.1)

سوال نمبر43 IPV4 :ایڈریس کی ایک مثال دیں۔

جواب192.168.1.1 :

سوال نمبر44:نشاندہی کریں کہ IPv4 ایڈریس299.53.2.2 درست ہے یا نہیں؟

جواب :یہ IPv4 ایڈریس درست **نہیں** ہے، کیونکہ IPv4 ایڈریس کے ہر حصے (octet) کی قدر0 سے255 کے درمیان ہونی چاہیے۔ یہاں پہلا حصہ 299 ہے، جو255 سے بڑا ہے۔

سوال نمبر45 IPv6 :کی ایک مثال لکھیں۔

جواب2001:0db8:85a3:0000:0000:8a2e:0370:7334 :

سوال نمبر46:ایچ ٹی ٹی پی کیا ہے؟

جواب HTTP (HyperText Transfer Protocol) **:**ایک پروٹوکول ہے جو انٹرنیٹ پر ویب پیجز کو منتقل کرنے کے لیے استعمال ہوتا ہے۔

سوال نمبر47:ڈی این ایس کا استعمال کیا ہے؟

جواب DNS (Domain Name System) **:**ڈومین ناموں (جیسے www.google.com) کو آئی پی ایڈریسز میں ترجمہ کرتا ہے، جس سے صارفین کے لیے ویب سائٹس تک رسائی آسان ہو جاتی ہے۔

سوال نمبر48:آئی پی ایڈریس اور ڈی این ایس کی ایک مثال دیں۔

جواب:

- **ڈومین نام(DNS):** www.google.com
- **آئی پی ایڈریس142.250.203.110 :**

سوال نمبر49:نیٹ ورکس میں استعمال ہونے والے چار پروٹوکز کے نام لکھیں۔

جواب:

1. TCP/IP (Transmission Control Protocol/Internet Protocol)
2. HTTP (HyperText Transfer Protocol)
3. FTP (File Transfer Protocol)
4. SMTP (Simple Mail Transfer Protocol)

سوال نمبر50:نیٹ ورک سیکیورٹی کیا ہے اور یہ کیوں ضروری ہوتی ہے؟

جواب: نیٹ ورک سیکیورٹی ان اقدامات پر مشتمل ہے جو ڈیٹا کی حفاظت اور کمپیوٹر نیٹ ورکس تک غیر مجاز رسائی کو روکنے کے لیے کیے جاتے ہیں۔ یہ ڈیٹا کی حفاظت، حملوں سے بچاؤ، اور رازداری کو برقرار رکھنے کے لیے ضروری ہے۔

سوال نمبر51: خفیہ کاری کیا ہوتی ہے؟

جواب: خفیہ کاری (Encryption) ڈیٹا کو ایک محفوظ فارمیٹ میں تبدیل کرنے کا عمل ہے جسے صرف درست ڈیکرپشن کلید رکھنے والے مجاز فریق ہی پڑھ یا سمجھ سکتے ہیں۔

سوال نمبر52: مضبوط پاسورڈ کیوں ضروری ہوتا ہے؟

جواب: مضبوط پاس ورڈ اس لیے ضروری ہے تاکہ صرف مجاز صارفین ہی نیٹ ورک کے وسائل تک رسائی حاصل کر سکیں اور غیر مجاز رسائی کو روکا جا سکے۔

سوال نمبر53: سیکیورٹی تھریٹ کیا ہوتے ہیں؟ سیکیورٹی نیٹ کو درپیش عام تھریٹ کی فہرست بنائیں۔

جواب: سیکیورٹی تھریٹ: یہ کوئی بھی ممکنہ خطرہ ہے جو کمپیوٹر سسٹم یا نیٹ ورک کو نقصان پہنچا سکتا ہے۔ **عام تھریٹس:**

- میلویئر (Malware)
- فشنگ (Phishing)
- ڈینائل آف سروس (DoS) حملے
- مین-ان-دی-مڈل حملے

سوال نمبر54: میلویئر کیا ہے؟

جواب: میلویئر (Malware) نقصان دہ سافٹ ویئر ہے جیسے وائرس، ورمز، اور رینسم ویئر جو ڈیٹا کو نقصان پہنچا یا چوری کر سکتا ہے۔

سوال نمبر55: جعل سازی کا مقصد کیا ہوتا ہے؟

جواب: جعل سازی (Phishing) کا مقصد صارفین کو دھوکہ دہی پر مبنی ای میلز یا ویب سائٹس کے ذریعے حساس معلومات، جیسے پاس ورڈ زیا کریڈٹ کارڈ کی تفصیلات، ظاہر کرنے پر آمادہ کرنا ہے۔

سوال نمبر56: ڈی او ایس حملہ کیا ہوتا ہے؟

جواب: ڈینائل آف سروس (Denial of Service - DoS) حملہ ایک نیٹ ورک کو ٹریفک سے بھر کر اس کے معمول کے کام میں خلل ڈالنے اور اسے ناقابل رسائی بنانے کی کوشش ہے۔

سوال نمبر57: سائفر ٹیکسٹ کیا ہوتا ہے؟ اس کو ڈکرپٹڈ کیسے کیا جا سکتا ہے؟

جواب: سائفر ٹیکسٹ (Ciphertext) انکرپٹ شدہ ڈیٹا کی شکل ہے۔ اسے ڈیکرپشن کلید (decryption key) کا استعمال کرتے ہوئے واپس اس کی اصل شکل (پلین ٹیکسٹ) میں تبدیل کیا جا سکتا ہے، اس عمل کو ڈیکرپشن کہتے ہیں۔

سوال نمبر58: ہیکنگ اور ہیکر کیا ہے؟

جواب:

- **ہیکنگ:** کسی کمپیوٹر سسٹم یا نیٹ ورک تک غیر مجاز رسائی حاصل کرنے کا عمل۔
- **ہیکر:** وہ شخص جو ہیکنگ کرتا ہے۔

سوال نمبر59: نیٹ ورکس کی عام اقسام کے نام لکھیں۔

جواب:

- پرسنل ایریا نیٹ ورک (PAN)
- لوکل ایریا نیٹ ورک (LAN)
- میٹروپولیٹن ایریا نیٹ ورک (MAN)
- وائڈ ایریا نیٹ ورک (WAN)

- کیمپس ایریانیٹ ورک(CAN)

سوال نمبر60 PAN : کو مثالوں کے ساتھ بیان کریں۔

جواب : پرسنل ایریانیٹ ورک (PAN) ایک چھوٹا نیٹ ورک ہے جو ذاتی آلات کے درمیان کم فاصلے پر مواصلات کے لیے استعمال ہوتا ہے۔ مثال: ایک اسمارٹ فون اور وائرلیس ہیڈ سیٹ کے درمیان بلوٹوتھ کنکشن۔

سوال نمبر61 LAN : کو مثالوں کے ساتھ بیان کریں۔

جواب : لوکل ایریانیٹ ورک (LAN) ایک محدود علاقے، جیسے گھر، اسکول، یا دفتر کی عمارت کے اندر کمپیوٹرز اور آلات کو جوڑتا ہے۔ مثال: آپ کے اسکول کی کمپیوٹر لیب میں تمام کمپیوٹرز کو جوڑنے والا نیٹ ورک۔

سوال نمبر62 WAN : کو مثالوں کے ساتھ بیان کریں۔

جواب : وائڈ ایریانیٹ ورک (WAN) ایک بڑے جغرافیائی علاقے پر محیط ہوتا ہے، جو متعدد LANs اور MANs کو جوڑتا ہے۔ مثال: انٹرنیٹ WAN کی سب سے بڑی مثال ہے۔

سوال نمبر63 CAN : کو مثالوں کے ساتھ بیان کریں۔

جواب : کیمپس ایریانیٹ ورک (CAN) ایک محدود جغرافیائی علاقے، جیسے یونیورسٹی کیمپس یا بزنس پارک کے اندر متعدد LANs کو جوڑتا ہے۔ مثال: ایک یونیورسٹی کے مختلف شعبوں اور عمارتوں کو جوڑنے والا نیٹ ورک۔

سوال نمبر64 LAN : اور WAN میں فرق کو مختصر بیان کریں۔

جواب LAN : ایک محدود علاقے (جیسے ایک عمارت) کا احاطہ کرتا ہے، جبکہ WAN ایک بڑے جغرافیائی علاقے (جیسے شہروں یا ممالک) پر پھیلا ہوتا ہے۔

سوال نمبر65: ورچوئل پرائیویٹ نیٹ ورک کیا ہوتا ہے؟

جواب : ورچوئل پرائیویٹ نیٹ ورک (VPN) ایک محفوظ کنکشن ہے جو عوامی نیٹ ورک (جیسے انٹرنیٹ) پر بنایا جاتا ہے۔ یہ آپ کے ڈیٹا کو انکرپٹ کر کے محفوظ بناتا ہے، خاص طور پر جب آپ عوامی وائی فائی استعمال کر رہے ہوں۔

سوال نمبر66: کمپیوٹر نیٹ ورک سسٹم کی چند حقیقی دنیا کی ایپلی کیشنز لکھیں۔

جواب:

- **کاروبار :** اندرونی مواصلات اور وسائل کا اشتراک۔
- **تعلیم :** آن لائن لرننگ پلیٹ فارمز اور تعلیمی وسائل تک رسائی۔
- **صحت کی دیکھ بھال :** مریضوں کی معلومات کا اشتراک اور ٹیلی میڈیسن۔

سوال نمبر67: صحت کی دیکھ بھال میں نیٹ ورکس کس طرح استعمال ہوتا ہے؟

جواب : صحت کی دیکھ بھال میں نیٹ ورکس مریضوں کی معلومات (Electronic Health Records - EHR) کے اشتراک، ٹیلی میڈیسن (دور سے علاج)، اور طبی ڈیٹا بیس تک رسائی کو آسان بناتے ہیں۔

سوال نمبر68: پروٹوکول کیا ہیں؟

جواب : پروٹوکولز ان قوانین اور ضوابط کا مجموعہ ہیں جو ڈیٹا مواصلات کو کنٹرول کرتے ہیں۔

سوال نمبر69: پروٹوکول کیوں ضروری ہیں؟

جواب : پروٹوکولز اس لیے ضروری ہیں تاکہ مختلف مینوفیکچررز کے آلات ایک دوسرے کے ساتھ قابل اعتماد طریقے سے بات چیت کر سکیں۔

سوال نمبر70 TCP/IP : کے بارے میں آپ کیا جانتے ہیں؟

جواب TCP/IP (Transmission Control Protocol/Internet Protocol) : انٹرنیٹ مواصلات کے لیے پروٹوکولز کا بنیادی مجموعہ ہے۔ TCP قابل اعتماد ڈیٹا کی منتقلی کو یقینی بناتا ہے، جبکہ IP ایڈریسنگ اور روٹنگ کو سنبھالتا ہے۔

سوال نمبر 71 TCP/IP: کس طرح انٹرنیٹ سے ڈیٹا منتقل کرتا ہے؟

جواب TCP/IP: ڈیٹا کو چھوٹے چھوٹے ٹکڑوں میں تقسیم کرتا ہے جنہیں "پیکٹس" کہا جاتا ہے۔ IP ہر پیکٹ کو اس کی منزل تک پہنچانے کے لیے روٹ کرتا ہے، اور TCP اس بات کو یقینی بناتا ہے کہ تمام پیکٹس صحیح ترتیب میں اور بغیر کسی غلطی کے منزل تک پہنچیں۔

سوال نمبر 72: پاکٹ سوئچنگ میں ڈیٹا کیسے ٹرانسفر کیا جاتا ہے؟

جواب: پیکٹ سوئچنگ میں، ڈیٹا کو پیکٹوں میں تقسیم کیا جاتا ہے۔ ہر پیکٹ کو آزادانہ طور پر نیٹ ورک کے ذریعے اس کی منزل تک بھیجا جاتا ہے، جہاں انہیں دوبارہ اصل ڈیٹا کی شکل میں جوڑا جاتا ہے۔

سوال نمبر 73: سرکٹ سوئچنگ موثر کیوں نہیں ہے؟

جواب: سرکٹ سوئچنگ اس لیے کم موثر ہے کیونکہ اس میں دو آلات کے درمیان ایک مخصوص مواصلاتی راستہ قائم کیا جاتا ہے جو پوری گفتگو کے دوران مختص رہتا ہے، چاہے ڈیٹا منتقل ہو رہا ہو یا نہیں۔ اس سے نیٹ ورک کے وسائل ضائع ہوتے ہیں۔

مشقی سوالات

سوال نمبر 1: ڈیٹا کمیونیکیشن کی وضاحت کریں اور اس کے اہم اجزاء کی فہرست بنائیں۔

جواب: ڈیٹا کمیونیکیشن: یہ ایک بھیجنے والے (sender) اور وصول کنندہ (receiver) کے درمیان ایک مواصلاتی میڈیم کے ذریعے ڈیٹا کا تبادلہ ہے۔

اہم اجزاء:

1. **بھیجنے والا (Sender):** وہ ڈیوائس جو ڈیٹا بھیجتی ہے۔
2. **وصول کنندہ (Receiver):** وہ ڈیوائس جو ڈیٹا وصول کرتی ہے۔
3. **پیغام (Message):** وہ ڈیٹا جو منتقل کیا جا رہا ہے۔
4. **پروٹوکول (Protocol):** قوانین کا مجموعہ جو مواصلات کو کنٹرول کرتا ہے۔
5. **میڈیم (Medium):** وہ طبعی یا وائرلیس راستہ جس کے ذریعے ڈیٹا سفر کرتا ہے۔

سوال نمبر 2: کمپیوٹر نیٹ ورکس میں روٹرز کے کردار کی وضاحت کریں۔

جواب: روٹرز کا بنیادی کردار مختلف نیٹ ورکس (جیسے آپ کا ہوم نیٹ ورک اور انٹرنیٹ) کو آپس میں جوڑنا ہے۔ وہ ڈیٹا پیکٹس کو ایک نیٹ ورک سے دوسرے نیٹ ورک تک ہدایت دینے کے ذمہ دار ہیں۔ راؤٹر ہر پیکٹ کے منزل کے آئی پی ایڈریس کو دیکھتا ہے اور اسے اپنی منزل تک پہنچانے کے لیے بہترین راستے کا تعین کرنے کے لیے راؤٹنگ ٹیبل کا استعمال کرتا ہے۔

سوال نمبر 3: پیکٹ سوئچنگ اور سرکٹ سوئچنگ کے درمیان فرق کی وضاحت کریں۔

جواب:

خصوصیت	سرکٹ سوئچنگ (Circuit Switching)	پیکٹ سوئچنگ (Packet Switching)
راستہ	ایک مخصوص، قائم شدہ راستہ ہوتا ہے۔	کوئی مخصوص راستہ نہیں ہوتا؛ ہر پیکٹ مختلف راستہ اختیار کر سکتا ہے۔
وسائل	وسائل پوری گفتگو کے لیے مختص رہتے ہیں۔	وسائل کا اشتراک کیا جاتا ہے اور ضرورت کے مطابق استعمال ہوتے ہیں۔
کارکردگی	کم موثر، کیونکہ خاموشی کے دوران بھی راستہ مختص رہتا ہے۔	زیادہ موثر، کیونکہ وسائل ضائع نہیں ہوتے۔
مثال	روایتی ٹیلی فون کال	انٹرنیٹ

سوال نمبر 4: نیٹ ورکس میں اسٹار ٹپالوجی استعمال کرنے کے فوائد کیا ہیں؟

جواب:

- **آسان انتظام:** مرکزی ڈیوائس (سوئچ) کی وجہ سے نیٹ ورک کا انتظام اور ٹربل شوٹنگ آسان ہے۔
- **قابل اعتمادی:** اگر ایک نوڈ یا کیبل ناکام ہو جائے تو باقی نیٹ ورک متاثر نہیں ہوتا۔

- **آسان توسیع :** نئے نوڈز کو مرکزی ڈیوائس سے جوڑ کر نیٹ ورک کو آسانی سے بڑھایا جا سکتا ہے۔

سوال نمبر5 OSI :ماڈل میں نیٹ ورک لیئر کے اہم افعال کیا ہیں؟

جواب : نیٹ ورک لیئر (لیئر 3) کا بنیادی کام مختلف نیٹ ورکس کے درمیان ڈیٹا کی منتقلی ہے۔ اس کے اہم افعال میں **روٹنگ** (ڈیٹا پیکٹس کے لیے بہترین راستے کا تعین کرنا) اور **لاجیکل ایڈریسنگ** (آئی پی ایڈریسز کا استعمال کرتے ہوئے آلات کی شناخت کرنا) شامل ہیں۔

سوال نمبر6 (DHCP) :کا مقصد کیا ہے؟

جواب (DHCP (Dynamic Host Configuration Protocol :کا مقصد ایک نیٹ ورک پر موجود آلات کو خود بخود آئی پی ایڈریس تفویض کرنا ہے۔ یہ نیٹ ورک کے انتظام کو آسان بناتا ہے کیونکہ منتظمین کو ہر ڈیوائس کے لیے دستی طور پر آئی پی ایڈریس کنفیگر کرنے کی ضرورت نہیں ہوتی۔

سوال نمبر7:ڈیٹا ٹرانسفر میں قابل اعتماد کے لحاظ سے TCP اور UDP کے درمیان فرق کریں۔

جواب:

- **TCP (Transmission Control Protocol):** یہ ایک قابل اعتماد پروٹوکول ہے۔ یہ اس بات کو یقینی بناتا ہے کہ تمام ڈیٹا پیکٹس صحیح ترتیب میں اور بغیر کسی غلطی کے منزل تک پہنچیں۔ یہ گمشدہ پیکٹوں کو دوبارہ بھیجتا ہے۔
- **UDP (User Datagram Protocol):** یہ ایک تیز، لیکن کم قابل اعتماد پروٹوکول ہے۔ یہ ڈیٹا بھیجتا ہے لیکن اس بات کی ضمانت نہیں دیتا کہ تمام پیکٹ پہنچیں گے یا صحیح ترتیب میں ہوں گے۔ یہ اسٹریمنگ اور آن لائن گیمنگ کے لیے استعمال ہوتا ہے جہاں رفتار زیادہ اہم ہے۔

سوال نمبر8:نیٹ ورک کی سیکیورٹی میں خفیہ کاری کی اہمیت کی وضاحت کریں۔

جواب : خفیہ کاری (Encryption) نیٹ ورک سیکیورٹی میں بہت اہم ہے کیونکہ یہ ڈیٹا کو ایک غیر پڑھنے کے قابل فارمیٹ میں تبدیل کر دیتی ہے۔ اس کا مطلب ہے کہ اگر کوئی غیر مجاز شخص ڈیٹا کو روک بھی لے، تو وہ اسے ڈیکرپشن کلید کے بغیر پڑھ نہیں سکتا۔ یہ حساس معلومات جیسے پاس ورڈز، مالیاتی تفصیلات، اور ذاتی پیغامات کو محفوظ رکھتی ہے۔

سوال نمبر9:فائروالز نیٹ ورکس کی حفاظت میں کس طرح کردار ادا کرتے ہیں؟

جواب : فائروالز ایک قابل اعتماد اندرونی نیٹ ورک اور ایک غیر معتبر بیرونی نیٹ ورک (جیسے انٹرنیٹ) کے درمیان ایک رکاوٹ کے طور پر کام کرتے ہیں۔ وہ پہلے سے طے شدہ سیکیورٹی قوانین کی بنیاد پر آنے والی اور جانے والی نیٹ ورک ٹریفک کی نگرانی اور اسے کنٹرول کرتے ہیں۔ وہ نقصان دہ ٹریفک کو روک کر نیٹ ورک کو غیر مجاز رسائی اور حملوں سے بچاتے ہیں۔

سوال نمبر10 encapsulation :نیٹ ورکس میں محفوظ کمیونیکیشن کو کیسے یقینی بناتا ہے؟

جواب : انکیپسولیشن (Encapsulation) وہ عمل ہے جس میں ڈیٹا کو پروٹوکول کی معلومات کے ساتھ لپیٹا جاتا ہے جب وہ OSI ماڈل کی مختلف تہوں سے گزرتا ہے۔ ہر تہہ اپنی ہیڈر کی معلومات شامل کرتی ہے، جس میں سورس اور منزل کے پتے جیسی تفصیلات ہوتی ہیں۔ یہ عمل ڈیٹا کو منظم کرتا ہے اور اس بات کو یقینی بناتا ہے کہ اسے صحیح طریقے سے روٹ کیا جائے اور منزل پر صحیح طریقے سے دوبارہ جوڑا جائے۔ اگرچہ انکیپسولیشن خود سیکیورٹی فراہم نہیں کرتی، لیکن یہ انکرپشن جیسے سیکیورٹی پروٹوکولز کو ڈیٹا کے ساتھ شامل کرنے کی اجازت دیتی ہے، جس سے محفوظ مواصلات ممکن ہوتے ہیں۔

اہم ترین انشائیہ سوالات

یونٹ 6: کمپیوٹر نیٹ ورکس کا تعارف

پیکٹ سوئچنگ اور سرکٹ سوئچنگ کا استعمال کرتے ہوئے کمپیوٹر نیٹ ورکس میں ڈیٹا کیسے منتقل ہوتا ہے اس کی وضاحت کریں۔

مختلف قسم کے نیٹ ورک ٹپالوجیز (star, ring, bus and mesh) کا موازنہ اور تقابل کریں۔

نیٹ ورک کی حفاظت کے مختلف طریقوں کا جائزہ لیں، بشمول فائروالز، خفیہ کاری اور اینٹی وائرس سافٹ ویئر۔

کاروبار، تعلیم اور صحت کی دیکھ بھال میں کمپیوٹر نیٹ ورکس کی حقیقی دنیا کی ایپلی کیشنز کی وضاحت کریں۔