

کمپیوٹر نیٹ ورکس



اس باب کا مطالعہ کرنے کے بعد طلبہ اس قابل ہو جائیں گے وہ:

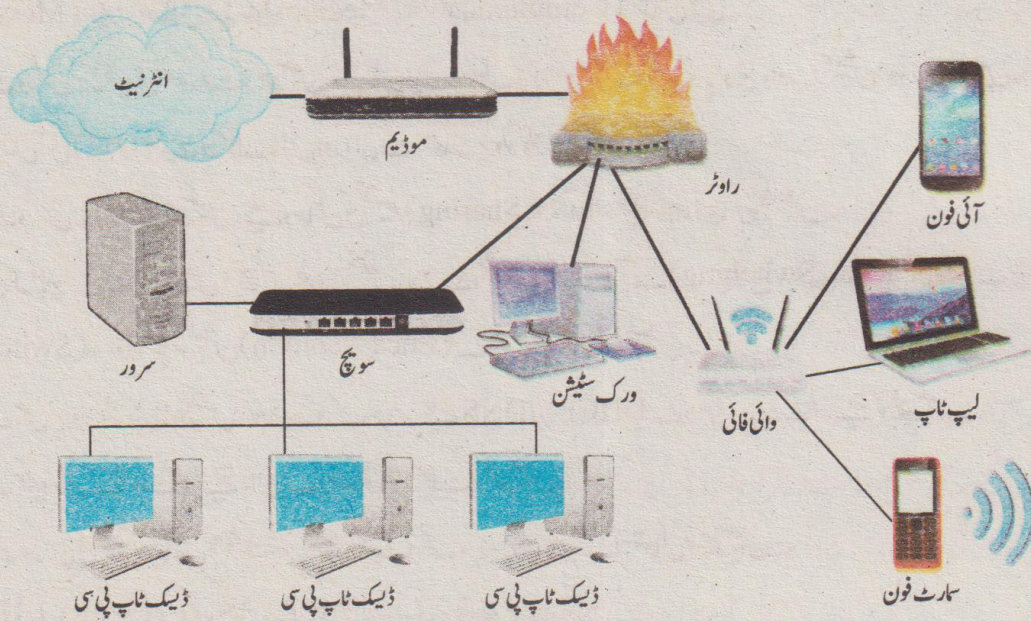
- کمپیوٹر نیٹ ورکس کو بطور سسٹم سمجھیں، ان کے مقاصد، اجزاء، اور ان اجزاء کے درمیان ڈیٹا کی ترسیل کو بیان کر سکیں۔
- ڈیٹا کمیونیکیشن کے بنیادی تصورات کو سمجھیں، جن میں پیغام بھیجنے والا (Sender)، وصول کنندہ (Receiver)، پروٹوکول (Protocol)، پیغام (Message)، اور مواصلاتی میڈیم (Communication Medium) شامل ہیں۔
- کمپیوٹر نیٹ ورکس کے کلیدی تصورات کو سمجھ سکیں، جن میں نیٹ ورکنگ ڈیوائسز، نیٹ ورک ٹوپالوجیز، اور ٹرانسمیشن موڈز شامل ہیں۔
- 7- لیئر او ایس آئی (OSI) نیٹ ورکنگ ماڈل اور اس سے متعلقہ پروٹوکولز کو سمجھ سکیں۔
- کمپیوٹر نیٹ ورکس کے فوائد کو سمجھ سکیں، جیسے وسائل کی تقسیم (Resource Sharing) اور ڈیٹا کمیونیکیشن۔
- یہ سمجھ سکیں کہ کمپیوٹر نیٹ ورکس میں ڈیٹا کس طرح منتقل ہوتا ہے، بشمول پیکٹ سوئچنگ (Packet Switching)، سرکٹ سوئچنگ (Circuit Switching)، اور انکپسولیشن (Encapsulation) کے ذریعے محفوظ کمیونیکیشن۔
- نیٹ ورک میں پروٹوکولز، ڈیٹا، پیکٹس، اور نیٹ ورک سروسز جیسے DNS اور DHCP کے کام کرنے کے طریقے کو سمجھ سکیں۔
- نیٹ ورک سیکورٹی کے مختلف طریقے، ان کے فوائد اور نقصانات کو سمجھ سکیں۔
- کمپیوٹر نیٹ ورکس کی حقیقی دنیا میں اپیلیکیشنز، مختلف نیٹ ورک سروسز، اور ان کے استعمال کو سمجھ سکیں۔
- ٹی سی پی / آئی پی (TCP/IP) کمیونیکیشن میں شامل معیاری پروٹوکولز کو جان سکیں۔
- نیٹ ورکنگ کے کلیدی اصطلاحات جیسے 7- لیئر او ایس آئی ماڈل، پیکٹ سوئچنگ، سرکٹ سوئچنگ، روٹر، DNS، UDP، IP، TCP/IP، DHCP، میزبان (Host)، براؤزرز، لیئرنگ، انکپسولیشن، اور مختلف پروٹوکولز کو جان سکیں۔
- ڈیٹا کمیونیکیشن کے اجزاء میں فرق کر سکیں۔
- نیٹ ورکنگ ڈیوائسز اور نیٹ ورک ٹوپالوجیز میں فرق کر سکیں۔
- ٹرانسمیشن موڈز میں فرق کر سکیں۔
- 7- لیئر او ایس آئی ماڈل کا استعمال کرتے ہوئے مختلف اقسام کے نیٹ ورکس کی شناخت اور وضاحت کر سکیں۔
- وضاحت کریں کہ ڈیٹا نیٹ ورکس میں کس طرح منتقل ہوتا ہے اور معیاری پروٹوکولز میں کون سے شامل ہیں۔
- پروٹوکولز، ڈیٹا، پیکٹس، اور نیٹ ورک سروسز جیسے DNS اور DHCP کے استعمالات کی وضاحت کر سکیں۔
- نیٹ ورک سیکورٹی کے مختلف طریقوں اور ان کے فوائد و نقصانات کی وضاحت کر سکیں۔

باب کا تعارف:

آج کی باہم جڑی ہوئی دنیا میں، کمپیوٹر نیٹ ورکس معاشرہ اور کاروباری اداروں کے کام کرنے میں ایک اہم کردار ادا کرتے ہیں۔ اس باب کا مقصد کمپیوٹر نیٹ ورکس کو سسٹم بشمول ان کے اجزاء، مقاصد، اور حقیقی دنیا کی ایپلی کیشنز کے طور پر جامع تفہیم فراہم کرنا ہے۔

6.1 نیٹ ورک بطور نظام

کمپیوٹر نیٹ ورک ایک دوسرے سے منسلک کمپیوٹرز اور آلات کا ایک نظام ہے جو کمیونیکیشن اور وسائل کو شیئر کر سکتا ہے۔ نیٹ ورکس چھوٹے، لوکل ایریا نیٹ ورک (LAN) سے لے کر بڑے علاقے کے نیٹ ورک (WAN) تک پھیلے ہو سکتے ہیں۔ نیٹ ورکس مختلف اجزاء پر مشتمل ہوتے ہیں جو کمیونیکیشن کو آسان بنانے کے لیے مل کر کام کرتے ہیں جیسا کہ شکل 6.1 میں دکھایا گیا ہے۔



شکل (6.1) نیٹ ورک ڈیاگرام

نیٹ ورک کے بنیادی اجزاء میں شامل ہیں:

- نوڈز (Nodes): ایسے آلات جو نیٹ ورک سے جڑے ہوئے ہیں، جیسے کمپیوٹر، اسمارٹ فون، اور پرنٹرز۔
- لنکس (Links): نوڈز کے درمیان کنکشن، جو وائرڈ یا وائرلیس ہو سکتے ہیں۔
- سوچ (Switch): ایسے آلات جو ڈیٹا فارورڈ کرنے کے لیے نیٹ ورک کے اندر متعدد نوڈز کو جوڑتے ہیں۔
- روٹرز (Router): ایسی ڈیوائسز جو مختلف نیٹ ورکس کو جوڑتی ہیں اور ان کے درمیان ڈیٹا پیکٹ کو ہدایت دیتی ہے۔

کیا آپ جانتے ہیں؟

انٹرنیٹ دنیا کا سب سے بڑا نیٹ ورک ہے جو کہ تمام نیٹ ورکس کو آپس میں جوڑتا ہے۔

سوچ استعمال کرنے کی مثال

- آفس نیٹ ورک میں فائل کی منتقلی کا تصور کریں۔ آپ اپنے کمپیوٹر سے کسی دوسرے کمرے میں کسی ساتھی کے کمپیوٹر پر ایک فائل بھیجتے

ہیں۔

- فائل کو پیکٹوں میں تقسیم کیا جاتا ہے اور ہر پیکٹ میں منزل کا میک ایڈریس (آپ کے ساتھی کے کمپیوٹر کا ایڈریس) ہوتا ہے۔
 - پیکٹوں کو نیٹ ورک سوئچ پر بھیجا جاتا ہے۔
 - سوئچ میڈیا ایکسیس کنٹرول (MAC) ایڈریس کی جانچ پڑتال کرتا ہے اور پیکٹوں کو صرف اسی پورٹ پر فارورڈ کرتا ہے جہاں آپ کے ساتھی کا کمپیوٹر منسلک ہے۔
 - ایک بار جب تمام پیکٹ موصول ہو جاتے ہیں تو، آپ کے ساتھی کا کمپیوٹر انھیں اصل فائل میں دوبارہ اکٹھا کرتا ہے۔
- مثال: ہوائی سفر کا نظام

ہوائی سفر کے ذریعے لوگوں کو بھیجنے کے بارے میں سوچیں۔ اس طرح سے ہوتا ہے۔

پیکٹ سوئچنگ (مسافر سفر):

- سفر کرتے وقت، مسافروں (ڈیٹا) کو گروپوں (پیکٹ) میں تقسیم کیا جاسکتا ہے اور مختلف پروازیں (راستے) تفویض کی جاسکتی ہیں۔
- پیکٹ سوئچنگ میں ہر گروپ کے پاس آخری منزل (آئی پی ایڈریس) کے ساتھ ایک ٹکٹ ہوتا ہے۔
- یہ گروپ حتمی منزل تک پہنچنے کے لیے مختلف ہوائی اڈوں (روٹز) کے ذریعے مختلف راستے اختیار کر سکتے ہیں۔

6.1.1 کمپیوٹر نیٹ ورکس کے مقاصد

کمپیوٹر نیٹ ورک کا بنیادی مقصد وسائل کا اشتراک، ڈیٹا کمیونیکیشن، ہم آہنگی کو یقینی بنانا ہے:

- وسائل کو شیئر کرنا: کمپیوٹر نیٹ ورکس ڈیوائسز کو وسائل کو شیئر کرنے کی سہولت دیتے ہیں، جیسے پرنٹرز اور اسٹوریج سے، اخراجات کو کم کرنا اور کارکردگی کو بہتر بنانا۔ مثال: ایک آفس نیٹ ورک میں، متعدد کمپیوٹر ایک ہی پرنٹر کو شیئر کر سکتے ہیں، جس سے متعدد پرنٹرز کی ضرورت کم ہو جاتی ہے۔
- ڈیٹا کمیونیکیشن: نیٹ ورک ڈیٹا سفر کی سہولت فراہم کرتے ہیں، ای میلز، فوری پیغام رسانی اور ویڈیو کانفرنسنگ کے ذریعے کمیونیکیشن کو ممکن بناتے ہیں۔ مثال: مختلف مقامات پر ملازمین زوم یا مائیکروسافٹ ٹیمز جیسے ویڈیو کانفرنسنگ ٹولز کے ذریعے تعاون کر سکتے ہیں۔

ہیں۔

- کنکٹیویٹی اور تعاون: نیٹ ورکس ڈیوائسز کو مربوط کرتے ہیں، جس سے ریہوٹ ایکس اور تعاون کی سہولت ملتی ہے، پیداواری صلاحیت اور کچک کو بہتر بنایا جاسکتا ہے۔ مثال: ایک ٹیم گوگل ڈرائیو جیسی کلاؤڈ پر مبنی خدمات کا استعمال کرتے ہوئے ریلی ٹائم میں مشترکہ دستاویز پر کام کر سکتی ہے۔

کیا آپ جانتے ہیں؟

ورلڈ وائیڈ ریپ کوئم برزلی نے 1989 میں بنایا جس نے ڈیٹا کی رسانی اور اشتراک میں انقلاب برپا کر دیا۔

6.2 ڈیٹا کمیونیکیشن میں بنیادی تصورات

ڈیٹا کمیونیکیشن میں پیغام رسانی کے ذریعے پیغام بھیجنے والے اور وصول کنندہ کے درمیان ڈیٹا کا تبادلہ شامل ہوتا ہے۔ بنیادی اجزاء میں مرسل، وصول کنندہ، پیغام، پروٹوکول، اور میڈیم شامل ہیں۔

6.2.1 ڈیٹا کمیونیکیشن کے اجزاء

یہ پانچ بنیادی اجزاء پر مشتمل ہے:

- (i) سینڈر: وہ آلہ جو ڈیٹا بھیجتا ہے۔ مثال: ایک کمپیوٹر ایک ای میل بھیج رہا ہے۔
- (ii) وصول کنندہ: وہ آلہ جو ڈیٹا وصول کرتا ہے۔ مثال: ای میل وصول کرنے والا اسمارٹ فون۔
- (iii) پیغام: ڈیٹا جس کا تبادلہ کیا جا رہا ہے۔ مثال: ای میل کا مواد۔
- (iv) پروٹوکول: ڈیٹا کمیونیکیشن کرنے والے قواعد کا ایک مجموعہ۔ مثال: ویب کمیونیکیشن کے لیے استعمال ہونے والا ایچ ٹی ٹی پی پروٹوکول۔
- (v) میڈیم: وائرڈ یا وائرلیس راستہ جس کے ذریعے ڈیٹا سفر کرتا ہے۔ مثال کے طور پر: ایئر نیٹ کیبل یا وائی فائی۔

6.3 نیٹ ورکنگ ڈیوائسز

نیٹ ورکنگ ڈیوائسز میں ہب، روترز، سوئچز اور ایکسس پوائنٹس شامل ہیں۔ نیٹ ورک ٹریفک کے انتظام اور ڈیٹا کے بہاؤ میں ہر آلہ ایک مخصوص کردار ادا کرتا ہے۔

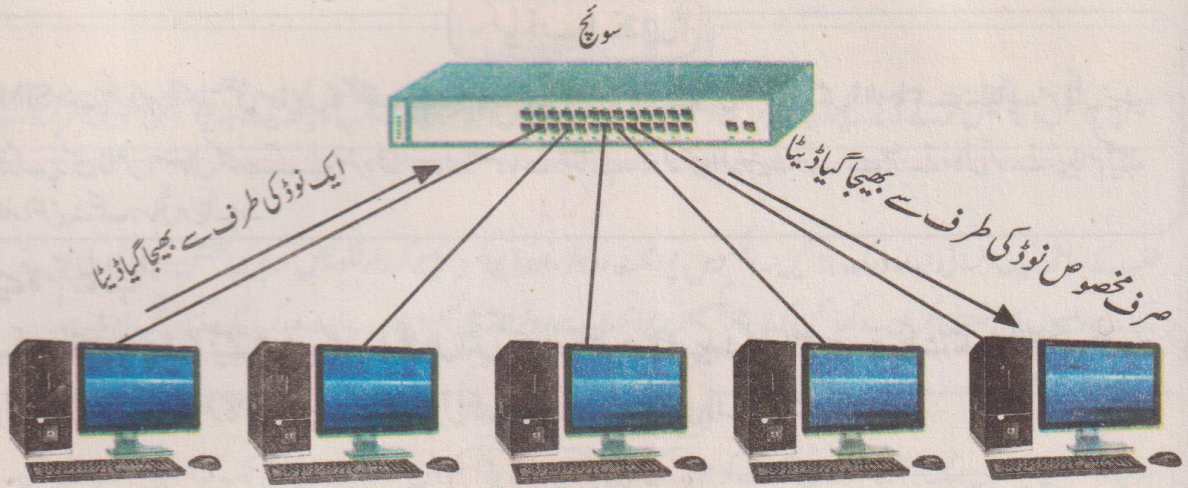
6.3.1 سوئچ (Switch)

سوئچ ایک نیٹ ورک کا آلہ ہے جو ایک ہی نیٹ ورک کے اندر متعدد آلات (جیسے کمپیوٹرز، پرنٹرز اور سرورز) کو جوڑتا ہے اور ان آلات کو ایک دوسرے کے ساتھ مؤثر طریقے سے رابطہ کرنے کی سہولت دیتا ہے۔ سوئچ ڈیٹا کی ٹریفک کو مؤثر طریقے سے منظم کر کے درست معلومات کے تبادلے کو یقینی بنا کر جدید نیٹ ورکس میں اہم کردار ادا کرتے ہیں۔ سوئچ کیسے کام کرتا ہے؟

ایک سوئچ او ایس آئی ماڈل کی ڈیٹا لنک لیئر (لیئر 2) پر کام کرتا ہے (سیکشن 6.6 دیکھیں)۔ یہ ڈیٹا کو صحیح ڈیوائس پر فارورڈ کرنے کے لیے میک (میڈیا ایکسیس کنٹرول) ایڈریس کا استعمال کرتا ہے۔ جب کوئی ڈیٹا پیکٹ سوئچ پر آتا ہے تو، یہ اس کی منزل کے میک ایڈریس کو پڑھتا ہے اور پیکٹ کو تمام آلات پر نشر کرنے کے بجائے صرف اس ایڈریس والے ڈیوائس پر بھیجتا ہے۔

دلچسپ معلومات:

پہلی بار سوئچ تمام منسلک ڈیوائسز کو ڈیٹا بھیجتا ہے اور ایک دفعہ جب اسے ایڈریس کا پتا چل جاتا ہے پھر یہ اسی کو ڈیٹا بھیجتا ہے۔



شکل 6.3: ایک نیٹ ورک سوچ جو متعدد آلات کو جوڑتا ہے

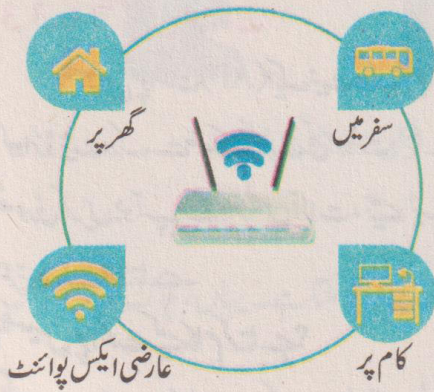
کیا آپ جانتے ہیں؟

سوچ ایک سمارٹ ٹریفک کنڈکٹر کی طرح ہوتا ہے۔ جو ٹریفک کو مطلوبہ منزل کی طرف بھیجتا ہے، جس سے نیٹ ورک تیز اور موثر انداز میں کام کرتا ہے۔

دلچسپ معلومات:

کیا آپ جانتے ہیں کہ گھریلو استعمال والے راؤٹر میں سوچ اور وائرلیس ایکس پوائنٹ ہوتے ہیں، جو ایک سے زیادہ آلات کو تاروں اور بغیر تاروں کے نیٹ ورک سے جوڑتا ہے۔

6.3.2 راؤٹر



موبائل، وائی فائی راؤٹر (شکل 6.2)

راؤٹر ایک نیٹ ورکنگ ڈیوائس ہے جو مختلف نیٹ ورکس کو یا ان سے منسلک آلات کو آپس میں جوڑتا ہے۔ یہ مختلف نیٹ ورکس پر ڈیٹا کے پیکٹس بھیجتا ہے۔ اس کو نیٹ ورک پہ ایک ٹریفک ڈائریکٹر کی طرح تصور کریں جو اس بات کو یقینی بناتا ہے کہ ڈیٹا ایک جگہ سے دوسری جگہ صحیح سلامت پہنچ گیا۔ شکل 6.2 دکھاتی ہے کہ ایک موبائل انٹرنیٹ کنکشن کس طرح ایک گھر کے نیٹ ورکس سے جڑتا ہے۔ اس کے متبادل کے طور پر ایٹھرنیٹ کی کیبل کو انٹرنیٹ تک رسائی اور گھر کے دوسرے آلات کو جوڑنے کے لیے استعمال کیا جاسکتا ہے۔ بڑے پیمانے پر مختلف قسم کے راؤٹرز استعمال کیے جاسکتے ہیں۔ (شکل 6.2)

کیا آپ جانتے ہیں؟

SIM سب سکر ایئر آئیڈنٹٹی موڈیول کا مخفف ہے۔ سم کارڈ ایک چھوٹا سا کارڈ ہے جس کو موبائل میں ڈالا جاتا ہے۔ یہ ایک موبائل نیٹ ورک پر کسی خاص استعمال کنندہ کے لیے منفرد شناخت اور معلومات رکھتا ہے۔ جو کہ کسی آلہ کو نیٹ ورک سے جڑنے، کال کرنے، پیغام بھیجنے اور انٹرنیٹ تک رسائی دیتا ہے۔

راؤٹر کیسے کام کرتا ہے؟

جب آپ انٹرنیٹ پر ڈیٹا بھیجتے ہیں تو یہ چھوٹے ٹکڑوں میں تقسیم ہو جاتا ہے جسے پیکٹ کہا جاتا ہے۔ ہر پیکٹ میں ڈیٹا کا ایک حصہ اور ایک حصہ منزل کا پتہ ہوتا ہے۔ راؤٹر کا کام ہر پیکٹ کو اپنی منزل تک پہنچنے کے لیے بہترین راستے کا تعین کرنا ہے۔

کیا آپ جانتے ہیں؟

راؤٹرز ڈیٹا پیکٹوں کے لیے بہترین راستے کا فیصلہ کرنے کے لیے راؤٹنگ ٹیبل استعمال کرتے ہیں۔ یہ ٹیبل ممکنہ راستوں کی فہرست دیتا ہے اور راؤٹر کو مؤثر فیصلے کرنے میں مدد کرتا ہے!

سرگرمی

ہیومن نیٹ ورک سرگرمی: کلاس میں طلباء کا استعمال کرتے: نئے ایک سادہ نیٹ ورک بنائیں۔ کمپیوٹر، روٹر اور ڈیٹا پیکٹ جیسے کردار تفویض کریں۔ ایٹھرنیٹ کیبلز کی نمائندگی کرنے کے لیے تاروں کا استعمال کریں اور طالب علموں کو تاروں کے ساتھ ایک گیند (ڈیٹا کی نمائندگی کرنے والی) پاس کریں تاکہ دیکھا جاسکے کہ روٹر ڈیٹا کو کس طرح ڈائریکٹ کرتا ہے۔

دلچسپ معلومات:

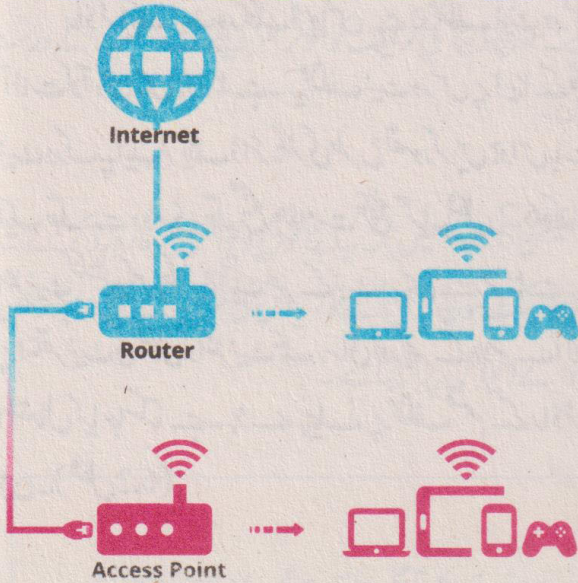
اپنے نیٹ ورک کو آسانی سے چلانے کے لیے، ہمیشہ اعلیٰ معیار کی ایٹھرنیٹ کیبلز کا استعمال کریں اور اس بات کو یقینی بنائیں کہ آپ کا سوئچ زیادہ گرم ہونے سے روکنے کے لیے ٹھنڈے، ہوادار علاقے میں رکھا گیا ہے۔

6.3.3 ایکسیس پوائنٹ

ایکسیس پوائنٹ (AP) ایک نیٹ ورک ڈیوائس ہے جو وائرلیس ڈیوائسز کو وائرڈ نیٹ ورک سے منسلک کرنے کی سہولت دیتا ہے۔ اسے ایک پل کے لیے تصوری کریں جو آپ کے وائرلیس آلات، جیسے لیپ ٹاپ اور اسمارٹ فون، کو انٹرنیٹ سے جوڑتا ہے۔

ایکسیس پوائنٹ کیسے کام کرتا ہے؟

ایکسیس پوائنٹ وائرڈ نیٹ ورک سے ڈیٹا وصول کر کے اور اسے وائرلیس طور پر آپ کے آلات پر منتقل کر کے کام کرتا ہے۔ یہ آپ کے وائرلیس آلات سے بھی ڈیٹا وصول کرتا ہے اور اسے وائرڈ نیٹ ورک کو بھیجتا ہے۔



شکل 6.4: ایک عام ایکسیس پوائنٹ

کیا آپ جانتے ہیں؟

ایکسیس پوائنٹس ڈیٹا منتقل کرنے کے لیے ریڈیو لہروں کا استعمال کرتے ہیں، بالکل اسی طرح جیسے آپ کا پسندیدہ ریڈیو اسٹیشن موسیقی نشر کرتا ہے!

سرگرمی

طلبہ کے ساتھ ایک انسانی نیٹ ورک بنائیں۔ ایکسیس پوائنٹ، روٹر، اور ڈیوائسز جیسے کردار تفویض کریں۔ کنکشن کی نمائندگی کرنے کے لیے رسیوں کا استعمال کریں۔ دکھائیں کہ ڈیٹا ایکسیس پوائنٹ سے روٹر اور پھر کسی دوسرے نیٹ ورک میں کیسے منتقل ہوتا ہے۔

کیا آپ جانتے ہیں؟

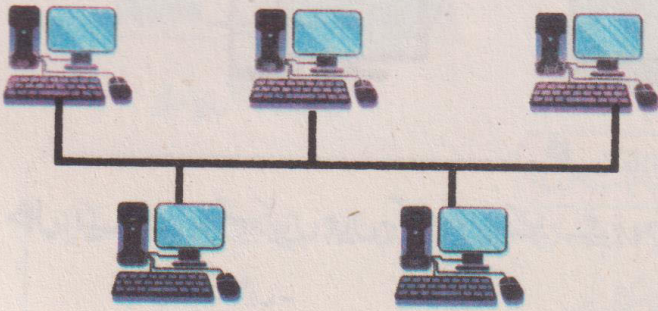
جدید ایکسیس پوائنٹس بیک وقت سینکڑوں آلات کو جوڑ سکتے ہیں، جس سے وہ اسکولوں، دفاتر اور یہاں تک کہ اسٹیڈیم کے لیے بھی بہترین بن جاتے ہیں؟

دلچسپ معلومات:

ایکسیس پوائنٹ ترتیب دیتے وقت، اپنے تمام آلات کے لیے بہترین کوریج اور سگنل کی طاقت کو یقینی بنانے کے لیے اسے مرکزی مقام پر رکھیں!

6.4 نیٹ ورک ٹپالوجیز

نیٹ ورک ٹپالوجیز کمپیوٹر سے مراد نیٹ ورک میں مختلف عناصر (لنکس، نوڈز، وغیرہ) کی ترتیب ہے جس میں ہر ڈیوائس کو ”نوڈ“ کہا جاتا ہے۔ ڈیوائسز کو ایک دوسرے سے منسلک کرنے کا طریقہ یہ ظاہر کرتا ہے کہ یہ آلات کس طرح آپس میں منسلک ہیں۔



شکل 6.5: بس ٹپالوجی

6.4.1 بس ٹپالوجی

بس ٹپالوجی میں، تمام آلات ایک ہی مواصلاتی لائن کو شیئر کرتے ہیں جسے بس کہا جاتا ہے۔ ہر آلہ اس مرکزی کیبل سے جڑا ہوا ہے۔

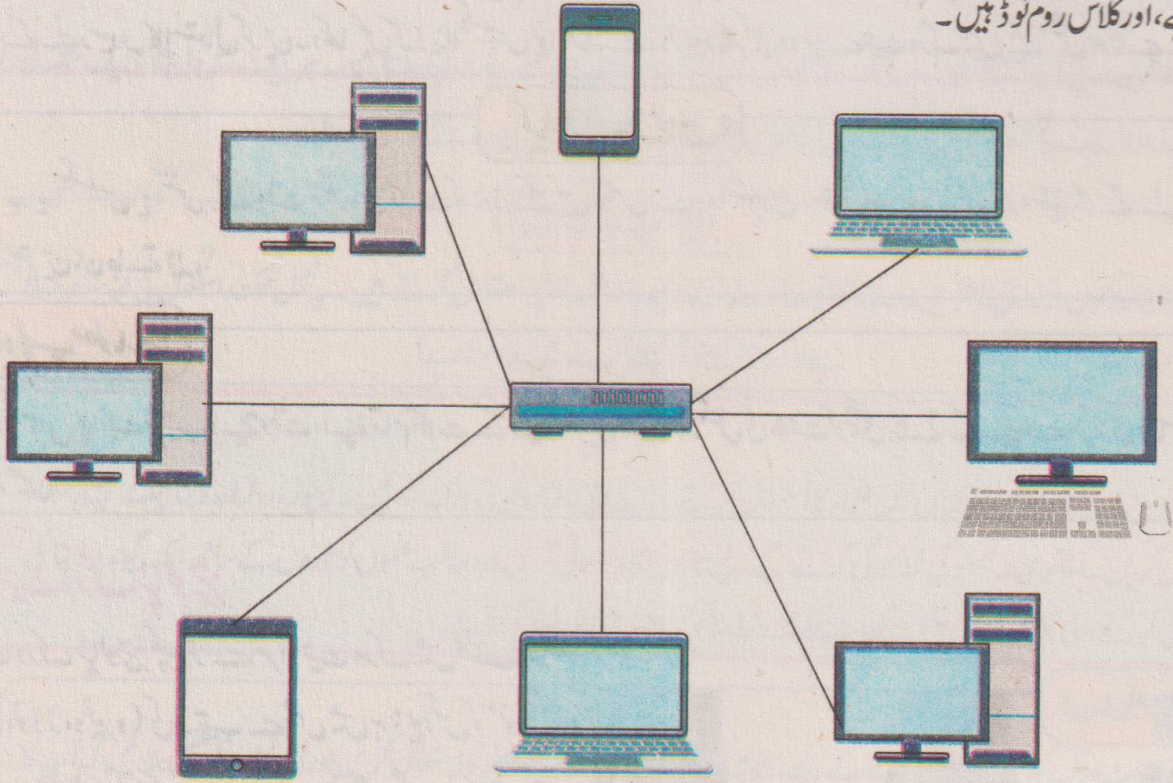
مثال: کلاس روم میں ایک وائٹ بورڈ کا تصور کریں جہاں ہر طالب علم استاد کے لکھے ہوئے نوٹ دیکھ سکتا ہے۔ یہاں، چاک بورڈ مشترکہ مواصلاتی لائن کی نمائندگی کرتا ہے۔

کیا آپ جانتے ہیں؟

بس ٹپالوجی بنانا آسان ہے لیکن اگر مین کیبل خراب ہو جاتی ہے تو پورا نیٹ ورک بند ہو جاتا ہے۔

6.4.2 اسٹار ٹپالوجی

اسٹار ٹپالوجی میں، تمام آلات ایک مرکزی ہب یا سوئچ سے منسلک ہوتے ہیں۔ ہب ڈیٹا کے بہاؤ کے لیے ریپیٹر کے طور پر کام کرتا ہے۔
مثال: ایک اسکول کے پرنسپل کے دفتر کے بارے میں تصور کریں جو انٹرکام کے ذریعے تمام کلاس رومز سے جڑا ہوا ہے۔ پرنسپل کا دفتر ہب ہے، اور کلاس روم نوڈ ہیں۔



شکل 6.6: اسٹار ٹپالوجی

مثال: ایک ایسے شہر کا تصور کریں جہاں ہر گھر سڑکوں کے ذریعے ہر دوسرے گھر سے براہ راست جڑا ہوا ہو۔ اگر ایک سڑک بند ہے، تو متعدد متبادل راستے ہیں۔

سرگرمی

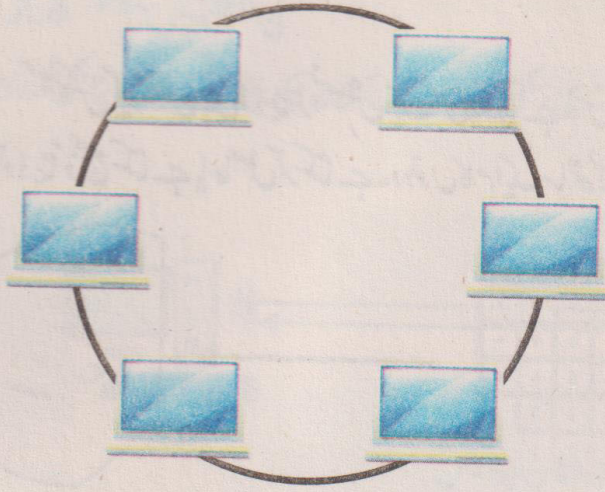
رسی اور پیپر کے کپس کو استعمال کرتے ہوئے اسٹار ٹپالوجی کا ماڈل بنائیں جو درمیانی سوئچ اور نوڈز کے درمیان کنکشن کو ظاہر کرے۔

کیا آپ جانتے ہیں؟

ہب نیٹ ورکنگ کا ایک ایسا آلہ ہے جو مختلف کمپیوٹنگ کے آلات کو لین (LAN) میں جوڑتا ہے۔ یہ ڈیٹا کو ہمیشہ براڈ کاسٹ کرتا ہے۔

6.4.3 رنگ ٹپالوجی

رنگ ٹپالوجی میں، ہر ڈیوائس دو اور ڈیوائسز سے ایک کیبل کے ذریعے منسلک ہوتی ہے اور ایک رنگ کی شکل بناتی ہے۔ اس میں ڈیٹا ایک

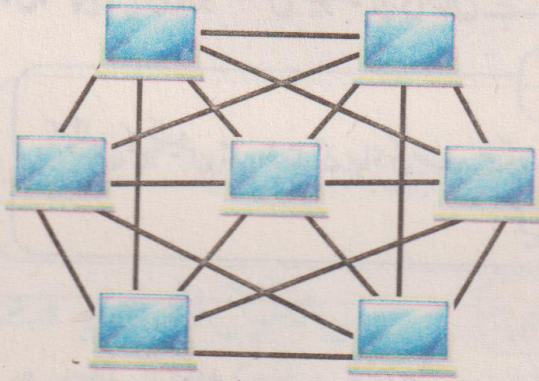


شکل (6.7) رنگ ٹپالوجی

ی سمت میں سفر کرتا ہے اور ایک سے دوسری ڈیوائس سے گزرتا ہے۔
مثال: ایک ریلے ریس پر غور کریں جہاں ہر دوڑنے والا ایک دائرے
میں اگلے ریز کو ایک ڈنڈا پاس کرتا ہے۔ جب تک کہ وہ دوبارہ
نقطہ آغاز تک نہ پہنچ جائے۔

دلچسپ معلومات

رنگ ٹپالوجی ہائی ٹریفک کو چلا سکتی ہے۔ لیکن اگر ایک کنکشن فیل ہو
جائے تو پورا نیٹ ورک متاثر ہوتا ہے۔ دوسرے رنگ نے اس
مسئلے کو کافی حد تک حل کر لیا ہے



شکل (6.8) میس ٹپالوجی

6.4.4 میس ٹپالوجی

میس ٹپالوجی میں، ہر آلہ ہر دوسرے آلے سے منسلک ہوتا ہے۔ یہ اعلیٰ
اور قابل اعتماد معیار فراہم کرتا ہے۔
مثال: ایک ایسے شہر کا تصور کریں جہاں ہر گھر سڑک کے ذریعے ہر دوسرے
گھر سے براہ راست جڑا ہوا ہو۔ اگر ایک سڑک بند ہے تو متعدد متبادل
راستے ہیں۔

کیا آپ جانتے ہیں؟

میس ٹپالوجی بہت قابل اعتماد ہے کیونکہ اگر ایک لنک ناکام ہو جاتا ہے تو، ڈیٹا کو دوسرے لنکس کے ذریعے ڈیٹا کو دوبارہ روٹ کیا
جاسکتا ہے۔

سرگرمی

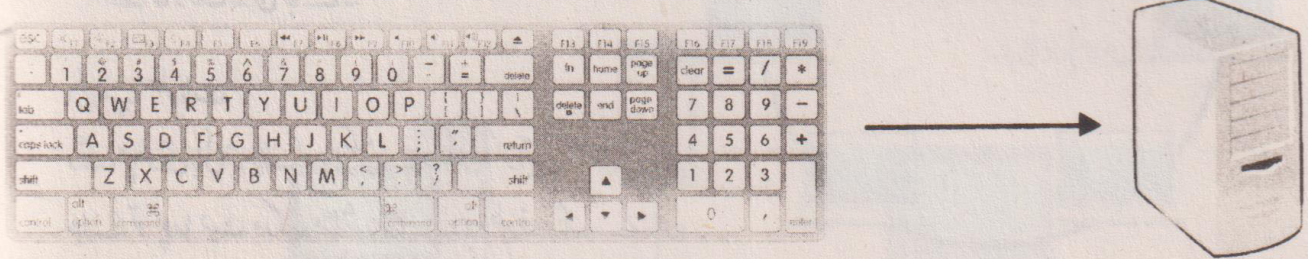
ٹپالوجی میں سے کسی ایک کا استعمال کرتے ہوئے اپنا نیٹ ورک ڈیاگرام بنائیں اور وضاحت کریں کہ ڈیٹا کس طرح ایک ڈیوائس سے
دوسرے میں سفر کرتا ہے۔

6.5 ٹرانسمیشن کے طریقے

نیٹ ورک میں کمیونیکیشن کے طریقے یہ وضاحت کرتے ہیں کہ آلات کے درمیان ڈیٹا کیسے منتقل ہوتا ہے۔ اس کے تین بنیادی طریقے
ہیں: سمپلکس، ہاف ڈوپلکس اور فل ڈوپلکس۔

6.5.1 سمپلیکس کمیونیکیشن

سمپلیکس کمیونیکیشن میں، ڈیٹا ٹرانسمیشن یک سمتی ہوتی ہے، جس کا مطلب ہے کہ یہ صرف ایک سمت میں بہہ رہا ہے۔ اس موڈ میں ایک آلہ یا تو ڈیٹا کو بھیج سکتا ہے یا حاصل کر سکتا ہے۔ دونوں کام ایک ساتھ نہیں کر سکتا۔



شکل 6.9: سمپلیکس کمیونیکیشن

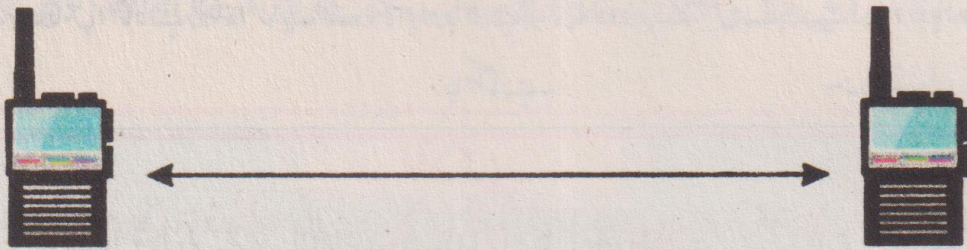
مثال: کمپیوٹر پر کی بورڈ سمپلیکس کمیونیکیشن کی مثال ہے۔

کیا آپ جانتے ہیں؟

سمپلیکس کمیونیکیشن میں، ڈیٹا کے بہاؤ کی سمت طے کی جاتی ہے، جس سے یہ اپیلی کیشنز کے لیے مفید ہو جاتا ہے جہاں صرف ایک طرف کمیونیکیشن کی ضرورت ہوتی ہے!

6.5.2 ہاف ڈوپلکس کمیونیکیشن

ہاف ڈوپلکس کمیونیکیشن میں، ڈیٹا ٹرانسمیشن دونوں سمتوں میں ہو سکتی ہے، لیکن بیک وقت نہیں۔ ایک ڈیوائس کو شروع ہونے سے پہلے دوسرے کے ٹرانسمیشن ختم ہونے کا انتظار کرنا ہوگا۔



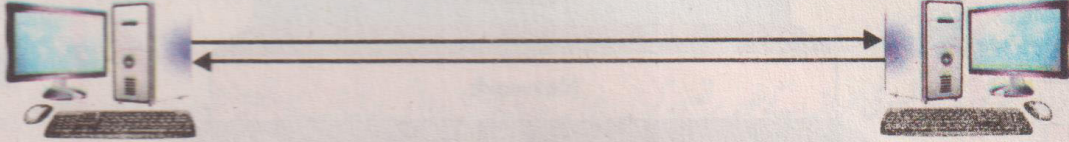
شکل (6.10) ہاف ڈوپلکس کمیونیکیشن

سرگرمی

ہاف ڈوپلکس کمیونیکیشن کا مظاہرہ کرنے کے لیے وائی ٹاکی یا کھلونائی فون کا استعمال کریں۔ طالب علموں کو باری باری بولنے اور سننے دیں۔

6.5.3 فل ڈوپلیکس کمیونیکیشن

فل ڈوپلیکس کمیونیکیشن میں، ڈیٹا ٹرانسمیشن بیک وقت دونوں سمتوں میں ہو سکتی ہے۔ دونوں آلات ایک ہی وقت میں ڈیٹا بھیج اور وصول کر سکتے ہیں۔



شکل (6.11) فل ڈوپلیکس کمیونیکیشن

مثال: ٹیلی فون گفتگو فل ڈوپلیکس کمیونیکیشن کی ایک مثال ہے۔ دونوں لوگ اپنی باری باری کا انتظار کیے بغیر ایک ہی وقت میں بات اور سن سکتے ہیں۔

دلچسپ معلومات:

فل ڈوپلیکس کمیونیکیشن ڈیٹا کی منتقلی کو زیادہ موثر بناتی ہے، جو جدید مواصلاتی نظام جیسے انٹرنیٹ براؤزنگ اور ویڈیو کالز کے لیے آئیڈیل ہے۔

کیا آپ جانتے ہیں؟

پہلے ٹیلی فونز ہاف ڈوپلیکس تھے، جہاں صرف ایک شخص بیک وقت بول سکتا تھا۔ جدید ٹیلی فونز فل ڈوپلیکس کو استعمال کرتے ہیں، جو دونوں لوگوں کو بیک وقت بات کرنے اور سننے کی اجازت دیتا ہے!

سرگرمی

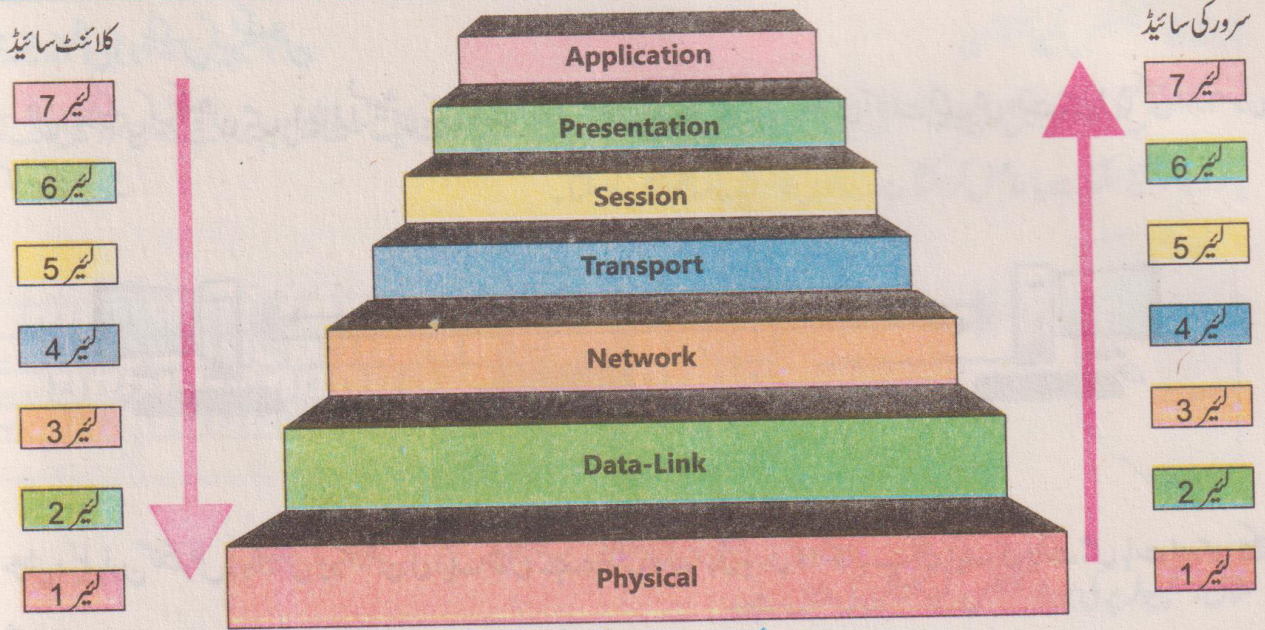
ہر کمیونیکیشن موڈ کا خاکہ کھینچیں اور ڈیٹا کے بہاؤ کی سمت کو نشان زد کریں۔ اپنے خاکوں کی کلاس کو وضاحت کریں۔

کیا آپ جانتے ہیں؟

پہلا پیغام جو ARPANET، جو انٹرنیٹ کا پیشرو تھا، پر بھیجا گیا، وہ "LO" تھا۔ اس کا مطلب "LOGIN" ہونا تھا، لیکن سسٹم نے پہلے دو حروف کے بعد کریش کر دیا۔

6.6 OSI نیٹ ورکنگ ماڈل

اوپن سسٹم انٹرکونکشن (OSI) ماڈل ایک فریم ورک ہے جو یہ سمجھنے کے لیے استعمال ہوتا ہے کہ مختلف نیٹ ورکنگ پروٹوکول کس طرح تعامل کرتے ہیں۔ اس میں 7 لیئر ہیں، ہر ایک کا ایک مخصوص فنکشن ہے۔ آئیے ان لیئرز کو مثالوں کے دیکھیں اور انہیں روزمرہ زندگی سے منسلک کریں۔



شکل 6.12: او ایس آئی ماڈل

لیئر 1: فزیکل لیئر

فزیکل لیئر آلات کے مابین فزیکل رابطے کے لیے ذمہ دار ہے۔ یہ ایک فزیکل میڈیم پر خام ڈیٹا بس کی ٹرانسمیشن سے متعلق ہے۔ مثال: کمپیوٹرز کو جوڑنے والے ہارڈ ویئر کا تصور کریں، جیسے نیٹ ورک انٹرفیس کیبلز، ریپیٹرز، ہب اور کنکٹرز۔

کیا آپ جانتے ہیں؟

فزیکل لیئر میں کیبل سے لے کر وٹچ لیول تک ہر وہ چیز شامل ہے جو ڈیٹا کی منتقلی میں استعمال ہوتی ہے۔

لیئر 2: ڈیٹا لنک لیئر

ڈیٹا لنک لیئر نوڈ سے نوڈ تک ڈیٹا ٹرانسفر اور غلطی کا پتہ لگانے اور اصلاح کے لیے ذمہ دار ہے۔ یہ اس بات کو یقینی بناتا ہے کہ فزیکل لیئر سے بھیجا گیا ڈیٹا غلطی سے پاک ہے۔

مثال: ڈیٹا لنک لیئر کو چوراہوں پر ٹریفک لائٹس کے طور پر تصور کریں، جو کاروں (ڈیٹا) کے بہاؤ کا انتظام کرتی ہیں اور تصادم کو روکتی ہیں۔

سرگرمی

آلات کے ساتھ ایک سادہ نیٹ ورک بنائیں اور فزیکل کنکشن اور ڈیٹا لنک لیئر کی ذمہ داریوں کو لیبل کریں۔

لیئر 3: نیٹ ورک لیئر

نیٹ ورک لیئر مختلف نیٹ ورکس کے درمیان ڈیٹا کی منتقلی کے لیے ذمہ دار ہے۔ یہ ماخذ سے منزل تک سفر کرنے کے لیے بہترین راستے کا تعین کرتی ہے۔

مثال: تصور کریں کہ ایک GPS سسٹم آپ کے لیے گھر سے اسکول تک سفر کرنے کے لیے بہترین راستہ تلاش کرتا ہے۔

دلچسپ معلومات:

نیٹ ورک لیئر نیٹ ورک کے درمیان ڈیٹا بھیجنے کے لیے IP ایڈریسز کا استعمال کرتی ہے۔

لیئر 4: ٹرانسپورٹ لیئر

ٹرانسپورٹ لیئر اس بات کو یقینی بناتی ہے کہ ڈیٹا کو سوس اینڈ سسٹم (End System) پر دوبارہ چلانے والے ایک عمل سے End System پر ایک عمل میں منتقل کیا جائے۔ یہ ڈیٹا کے بہاؤ کو کنٹرول اور غلطی کی جانچ پڑتال کا انتظام کرتی ہے۔
مثال: ٹرانسپورٹ لیئر کو ایک ڈیویری سروس کے طور پر تصور کریں جو اس بات کو یقینی بناتی ہے کہ آپ کا پیکیج محفوظ اور وقت پر پہنچ جائے۔

کیا آپ جانتے ہیں؟

ٹرانسپورٹ لیئر پروٹوکولز جیسے ٹرانسمیشن کنٹرول پروٹوکول (TCP) کا استعمال کرتا ہے تاکہ ڈیٹا کی منتقلی کو قابل اعتماد بنایا جاسکے!

لیئر 5: سیشن لیئر

سیشن لیئر اپیلی کیشنز کے درمیان سیشنز کا انتظام کرتی ہے۔ اس کا کام آلات کے مابین رابطے کو قائم کرنا، اس کو برقرار رکھنا اور ختم کرنا ہے۔
مثال: ایک فون کال کا تصور کریں جہاں سیشن کی لیئر کال کو ترتیب دیتی ہے، اسے منسلک رکھتی ہے، اور جب آپ ہنگ اپ کرتے ہیں تو اسے ختم کرتی ہے۔

سرگرمی

ایک فون کال کا کردار ادا کریں اور اس بات پر تبادلہ خیال کریں کہ سیشن کو کس طرح قائم کیا جاتا ہے، برقرار رکھا جاتا ہے اور ختم کیا جاتا ہے۔

لیئر 6: پریزنٹیشن لیئر

پریزنٹیشن لیئر اپیلی کیشن لیئر اور نیٹ ورک سسٹم کے درمیان ڈیٹا کا ترجمہ کرتی ہے۔ یہ ڈیٹا کو فارمیٹ اور Encrypt کرتی ہے تاکہ یہ یقینی بنایا جاسکے کہ یہ وصول کرنے والے سسٹم کے ذریعے پڑھنے کے قابل ہے۔
مثال: پریزنٹیشن لیئر کو ایک مترجم کے طور پر تصور کریں جو کسی کتاب کو ایک زبان سے دوسری زبان میں تبدیل کرتی ہے تاکہ زیادہ سے زیادہ لوگ اسے پڑھ سکیں۔

کیا آپ جانتے ہیں؟

پریزنٹیشن لیئر ڈیٹا کی انکرپشن اور کمپریشن کو ہینڈل کرتی ہے۔

لیئر 7: اپیلی کیشن لیئر

اپیلی کیشن لیئر End User کے قریب ترین لیئر ہے۔ یہ براہ راست اپیلی کیشنز کو نیٹ ورک کی خدمات فراہم کرتا ہے، جیسے ای میل، ویب براؤزنگ اور فائل ٹرانسفر وغیرہ۔

مثال: اپیلی کیشن لیئر کا تصور کریں جیسے ایک ویڈیو آپ کا آرڈر کسی ریستوران میں لیتا ہے اور آپ کا کھانا لاتا ہے۔

سرگرمی

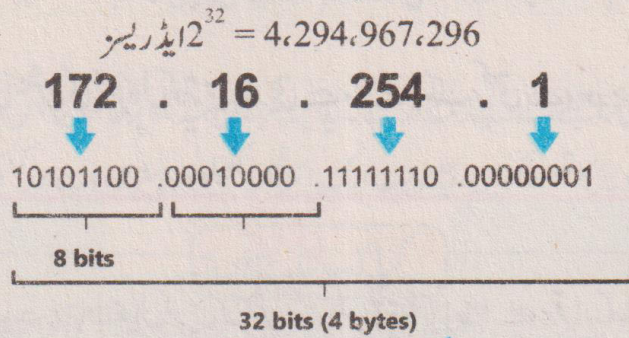
ان ایپلی کیشنز کی فہرست بنائیں جو آپ روزانہ استعمال کرتے ہیں اور شناخت کریں کہ نیٹ ورک خدمات کے لیے ایپلی کیشن لیئر پر انحصار کرتے ہیں۔

6.7 IPv6 اور IPv4

انٹرنیٹ پروٹوکول (IP) انٹرنیٹ سے منسلک آلات کو تفویض کردہ منفرد شناخت کنندہ ہیں۔ اس کے دو بنیادی ورژن ہیں: IPv4 اور IPv6۔ آئیے مثالوں کے ذریعے ان کے درمیان فرق دیکھتے ہیں اور روزمرہ کی زندگی سے منسلک کرتے ہیں۔

6.7.1 IPv4 (انٹرنیٹ پروٹوکول ورژن 4)

IPv4 انٹرنیٹ پروٹوکول کا چوتھا ورژن ہے اور آج سب سے زیادہ وسیع پیمانے پر استعمال ہوتا ہے۔ یہ 32 بت ایڈریس اسکیم استعمال کرتا ہے، جس سے تقریباً 4.3 بلین منفرد ایڈریسز بنتے ہیں۔ منفرد IPv4 ایڈریسز کی کل تعداد تلاش کرنے کے لیے ہم 2^{32} کا حساب لگاتے ہیں، جو 32 بتس کے تمام ممکنہ امتزاج کی نمائندگی کرتا ہے۔ یعنی:



شکل IPv4:6.13 ایڈریس فارمیٹ

کیا آپ جانتے ہیں؟

IPv4 ایڈریس کو چار حصوں میں لکھا جاتا ہے، ہر حصے کا نمبر 0 سے 255 تک ہوتا ہے (مثال کے طور پر، 1.1.168.192)۔

6.7.1 IPv6

IPv6 انٹرنیٹ پروٹوکول کا تازہ ترین ورژن ہے جو IPv4 کی جگہ لینے کے لیے ڈیزائن کیا گیا ہے۔ یہ 128 بت ایڈریس اسکیم کا استعمال کرتا ہے، جس سے منفرد ایڈریسز کی تقریباً لامحدود تعداد کی سہولت ملتی ہے۔

مثال: ڈیجیٹل فنکر پرنٹ کی طرح آئی پی وی 6 ایڈریس کا تصور کریں۔ یہ نہ صرف سڑک پر گھروں کے لیے بلکہ ساحل سمندر پر ریت کے ہر دانے کے لیے ایک انوکھا شناخت فراہم کر سکتا ہے۔ مثال کے طور پر:

2001:0000:130F:0000:0000:0900:876A:130B

کیا آپ جانتے ہیں؟

IPv6 کو IPv4 کی خامیاں دور کرنے کے لیے ڈیزائن کیا گیا تھا جو کہ انٹرنیٹ کی بہت تیزی سے بڑھتی ہوئی مقبولیت کی وجہ سے ظاہر ہوئی تھیں۔

6.8 پروٹوکول اور نیٹ ورک کی خدمات

6.8.1 پروٹوکول کا تعارف

پروٹوکول قوانین کے سیٹ ہیں جو ڈیٹا کمیونیکیشن کو کنٹرول کرتے ہیں۔ عام پروٹوکول میں SMTP اور FTP، HTTP، TCP/IP شامل ہیں۔

مثال: ہائپر ٹیکسٹ ٹرانسفر پروٹوکول (HTTP) انٹرنیٹ پر ویب صفحات کی منتقلی کے لیے استعمال ہوتا ہے۔

6.8.2 DNS اور DHCP نیٹ ورک

DNS ڈومین ناموں کو آئی پی ایڈریسز پر بھیجتا ہے جس سے صارفین کے لیے ویب سائٹس تک رسائی آسان ہو جاتی ہے۔
مثال: جب آپ براؤزر میں www.example.com ٹائپ کرتے ہیں تو، ڈی این ایس اسے متعلقہ آئی پی ایڈریس میں تبدیل کرتا ہے۔
ڈائنامک ہوسٹ کنٹرول پروٹوکول (DHCP)

DHCP نیٹ ورک مینجمنٹ کو آسان بناتے ہوئے خود بخود نیٹ ورک پر موجود ڈیوائسز کو IP ایڈریس تفویض کرتا ہے۔

مثال: جب کوئی آلہ وائی فائی نیٹ ورک سے جڑتا ہے تو، DHCP اُس کو IP ایڈریس فراہم کرتا ہے۔

6.9 نیٹ ورک سیکورٹی

نیٹ ورک سیکورٹی میں ڈیٹا کی حفاظت اور کمپیوٹر نیٹ ورکس تک غیر مجاز رسائی کو روکنے کے اقدامات شامل ہیں۔ آئیے مثالوں کے ساتھ نیٹ ورک سیکورٹی کی اہمیت اور کچھ اہم تصورات دیکھتے ہیں۔

6.9.1 نیٹ ورک سیکورٹی کی اہمیت

نیٹ ورک کی حفاظت کئی وجوہات کی بنا پر اہم ہے:

- ڈیٹا پروٹیکشن: اس بات کو یقینی بنانا کہ حساس معلومات تک غیر مجاز صارفین کی طرف سے رسائی یا تبدیل نہیں کیا جاتا ہے۔
- حملوں کی روک تھام: بد نیتی پر مبنی حملوں کے خلاف دفاع جو نیٹ ورکس میں خلل ڈال سکتے ہیں اور ڈیٹا چوری کر سکتے ہیں۔
- رازداری کو برقرار رکھنا: ذاتی اور خفیہ معلومات کو سمجھوتہ ہونے سے بچانا
- دستیابی کو یقینی بنانا: اس بات کو یقینی بنانا کہ نیٹ ورک کے وسائل مجاز صارفین کے لیے دستیاب اور قابل رسائی ہیں۔

6.9.2 نیٹ ورک سیکورٹی میں اہم تصورات

فائر والز (Firewalls)

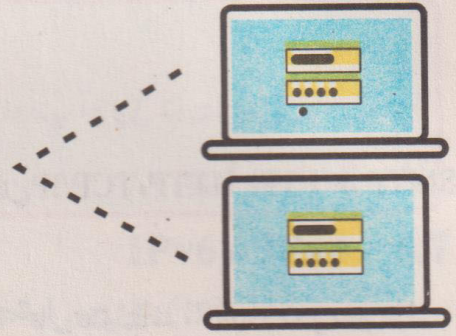
فائر والز سیکورٹی سسٹم ہیں جو پہلے سے طے شدہ سیکورٹی قوانین کی بنیاد پر آنے اور جانے والے نیٹ ورک ٹریفک کی نگرانی اور کنٹرول کرتے ہیں۔



1



2



3

تصویر 6.15: PAN: بلوٹوٹھ کنکشن

کیا آپ جانتے ہیں؟

فائر والز قابل اعتماد اندرونی نیٹ ورکس اور ناقابل اعتماد بیرونی نیٹ ورکس کے درمیان رکاوٹ کا کام کرتی ہیں، جیسے کہ سکیورٹی چیک پوائنٹ۔

خفیہ کاری (Encryption)

خفیہ کاری ڈیٹا کو ایک محفوظ شکل میں تبدیل کرتی ہے جسے صرف صحیح Decryption پر مجاز فریقوں کے ذریعے پڑھایا سمجھا جاسکتا ہے۔ Encryption خفیہ شدہ ڈیٹا کو اس کی اصل شکل میں واپس تبدیل کرنے کا عمل ہے۔

مثال: ایک سادہ ٹیکسٹ (Hello, World!)

مثال:

Encrypted ٹیکسٹ، جہاں سادہ متن میں ہر حرف کی جگہ اس حرف نے لے لی ہے جو حرف تہجی سے 3 پوزیشن آگے ہے۔

Khoor,Zroug

Decryption: الٹا اسی شفٹ سائفر کا استعمال کرتے ہوئے Khoor,Zroug کو Hello, Wordl میں تبدیل کرنا۔

ممالک کے درمیان سائفر ٹیکسٹ کا تبادلہ

ممالک اکثر خفیہ کاری کا استعمال کرتے ہوئے حساس معلومات کا محفوظ طریقے سے تبادلہ کرتے ہیں۔ خفیہ شدہ ڈیٹا، جسے سائفر ٹیکسٹ کے نام سے جانا جاتا ہے، صرف مطلوبہ وصول کنندہ کے ذریعے پڑھا جاسکتا ہے جس کے پاس Decryption کی Key ہے۔ یہ قومی سلامتی کو یقینی بناتا ہے اور خفیہ معلومات کو غیر مجاز جماعتوں کے ذریعے روکنے اور پڑھنے سے بچاتا ہے۔

سرکرمی

3 کی Key کے ساتھ شفٹ سائفر کا استعمال کرتے ہوئے ایک سادہ پیغام کو خفیہ کریں (ہر حرف حروف تہجی میں 3 مقام آگے منتقل کیا گیا ہے۔) اس کے بعد، اپنے ہم جماعتوں کے ساتھ پیغامات کا تبادلہ کریں اور ایک دوسرے کے پیغامات Decrypt کریں۔

کیا آپ جانتے ہیں؟

دوسری جنگ عظیم کے دوران، اتحادیوں نے اپنی کمیونیکیشن کو خفیہ کرنے کے لیے اینگما مشین کا استعمال کیا۔ جرمن اینگما خفیہ پیغامات کو ڈی کرپٹ کرنے کی صلاحیت نے ان کی فتح میں اہم کردار ادا کیا۔

دلچسپ معلومات:

حساس معلومات کی حفاظت کے لیے مضبوط خفیہ کاری الگورتھم کا استعمال کریں، جس سے یہ غیر مجاز صارفین کے لیے ناقابل مطالعہ ہو جاتا ہے۔

پاس ورڈ اور توثیق

پاس ورڈ اور توثیق کے طریقے اس بات کو یقینی بناتے ہیں کہ صرف مجاز صارفین ہی نیٹ ورک کے وسائل تک رسائی حاصل کر سکتے ہیں۔

سرگرمی

مضبوط پاس ورڈ کی اہمیت پر تبادلہ خیال کریں اور پاس ورڈ جزیئر کا استعمال کرتے ہوئے محفوظ پاس ورڈ بنانے کی مشق کریں۔

6.9.3 نیٹ ورک سکیورٹی کے لیے عام خطرات

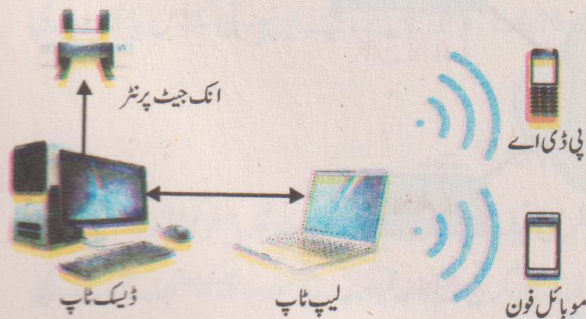
- (i) میلویئر (Malware): بدخواہ سافٹ ویئر جیسے وائرس، بگ اور رینسم ویئر جو ڈیٹا کو نقصان پہنچا سکتے ہیں یا ڈیٹا چوری کر سکتے ہیں۔
- (ii) جعل سازی (Phishing): دھوکہ دہی والی ای میلز یا ویب سائٹس کے ذریعے حساس معلومات ظاہر کرنے کے لیے صارفین کو دھوکہ دینے کی کوشش کرتی ہے۔
- (iii) ڈینائل سروس کے حملے (Denial of Service Attacks): ٹریفک کے ساتھ ایک نیٹ ورک کو اس کے معمول کے آپریشن میں خلل ڈالنے اور اسے غیر دستیاب بنانے کے لیے اس کا استعمال کیا جاتا ہے۔
- (iv) درمیان میں انسانی حملے (Man-in-the-Middle Attacks): معلومات چوری کرنے یا پیغامات کو تبدیل کرنے کے لیے دوفریقوں کے مابین کمیونیکیشن کو روکنا۔

6.10 نیٹ ورکس کی اقسام

نیٹ ورکس کو ان کے سائز، رینج اور مقصد کی بنیاد پر درجہ بندی کی جاتی ہے۔ آئیے کچھ عام قسم کے نیٹ ورکس کو دیکھتے اور سمجھتے ہیں۔

6.10.1 پرسنل ایریا نیٹ ورک (PAN)

PAN ایک چھوٹا سا نیٹ ورک ہے جو مختصر وقت میں ذاتی آلات، جیسے اسمارٹ فونز، ٹیبلیٹس اور لیپ ٹاپ کے مابین کمیونیکیشن کے لیے استعمال ہوتا ہے۔



شکل 6.15: پرسنل ایریا نیٹ ورک (PAN)

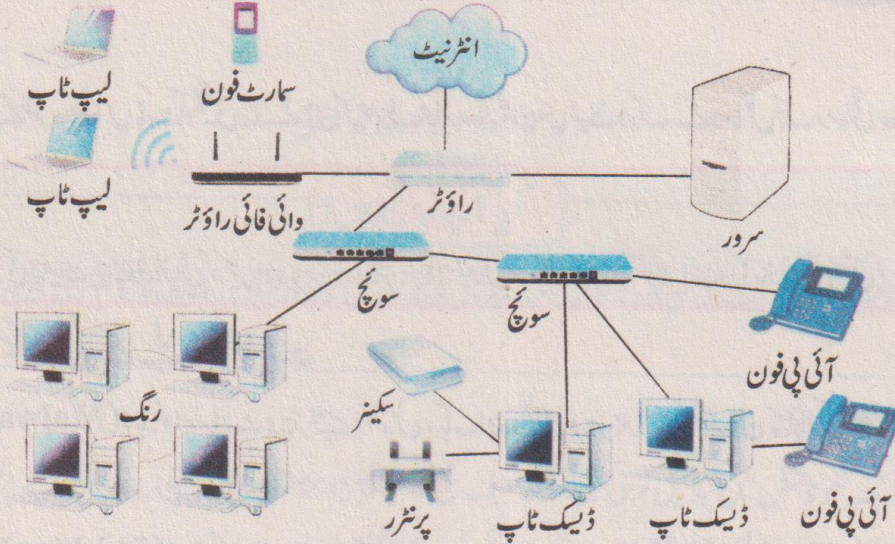
مثال: PAN: نیٹ ورک اسمارٹ فون اور وائرلیس ہیڈ سیٹ کے درمیان نیٹ ورک تشکیل دیتا ہے۔

کیا آپ جانتے ہیں؟

PAN کی رینج عمومی طور پر چند میٹر ہوتی ہے اور یہ پرسنل آلات کی کمیونیکیشن کے لیے بہترین ہے۔

لوکل ایریا نیٹ ورک (LAN)

LAN ایک ایریا نیٹ ورک ہے جو کمپیوٹرز اور آلات کو ایک محدود علاقے کے اندر جیسے گھر، اسکول یا دفتر کی عمارتوں کو جوڑتا ہے۔



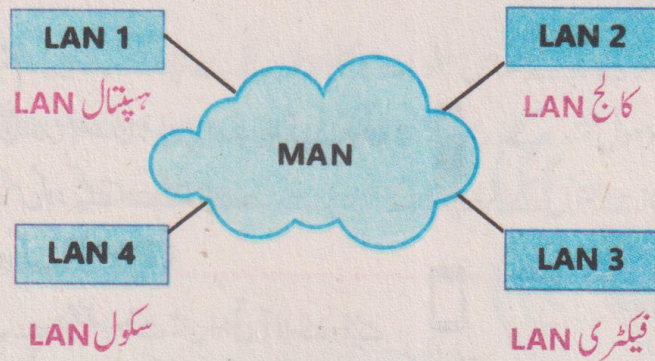
شکل (6.16) لوکل ایریا نیٹ ورک

سرگرمی

اسکول کے کمپیوٹر نیٹ ورک کا خاکہ بنائیں۔ جس میں آلات اور کنکشنز کو لیبل کریں۔

میٹر پولیٹن ایریا نیٹ ورک (MAN)

ایک بڑے کیمپس یا ایک شہر کی حد تک پھیلا ہوا نیٹ ورک جس میں کچھ LAN بھی ہو سکتے ہیں۔



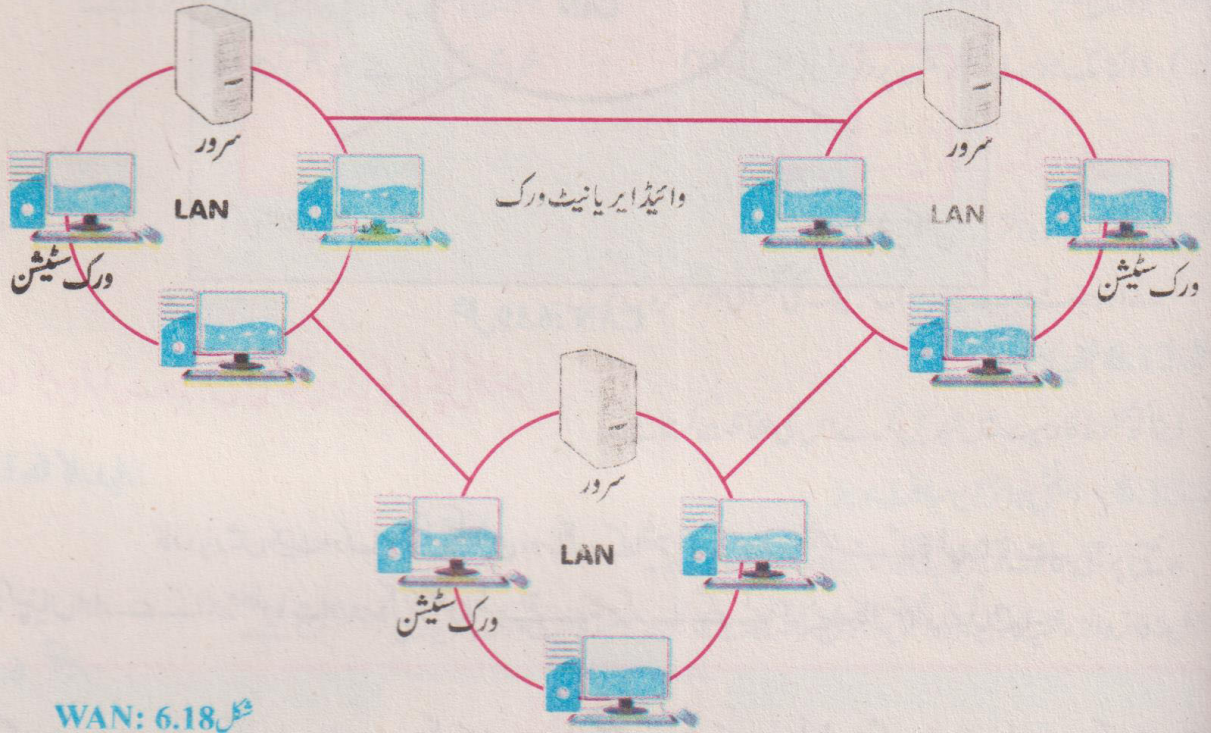
شکل 6.17: MAN

مثال: آپ کے اسکول میں کمپیوٹر نیٹ ورک جو لیبل میں تمام کمپیوٹرز کو جوڑتا ہے وہ LAN ہے۔

6.10.1 وائیڈ ایریا نیٹ ورک (WAN)

ایک WAN ایک بڑے جغرافیائی علاقے کا احاطہ کرتا ہے جو متعدد LAN اور MAN کو جوڑتا ہے۔ انٹرنیٹ WAN کی سب سے بڑی مثال ہے۔

مثال: وہ نیٹ ورک جو مالک میں ملٹی نیشنل کمپنی کے مختلف برانچ دفاتر کو جوڑتا ہے وہ WAN ہے۔



شکل 6.18: WAN

دلچسپ معلومات:

VPN کا استعمال کرتے ہوئے محفوظ طریقے سے WAN سے جڑیں اور عوامی نیٹ ورکس تک رسائی حاصل کرتے وقت اپنے ڈیٹا کی حفاظت کریں۔

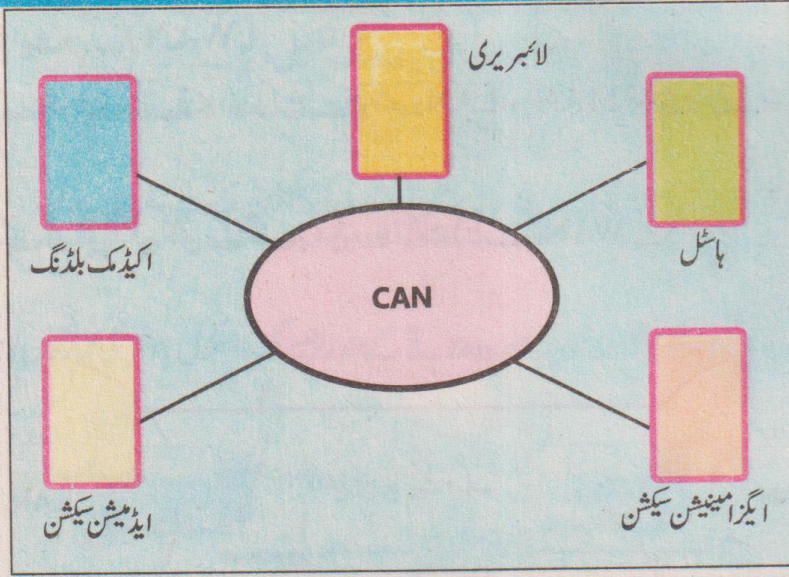
6.10.2 کیمپس ایریا نیٹ ورک (CAN)

CAN ایک ایسا نیٹ ورک ہے جو ایک محدود جغرافیائی علاقے کے اندر متعدد LAN کو جوڑتا ہے، جیسے یونیورسٹی کیمپس یا کاروباری پارک۔

مثال: وہ نیٹ ورک جو یونیورسٹی کے اندر مختلف محکموں اور عمارتوں کو جوڑتا ہے وہ ایک CAN ہے۔

مختلف قسم کے نیٹ ورکس کو سمجھنے سے ہمیں یہ سمجھنے میں مدد ملتی ہے کہ ڈیٹا کس طرح ایک ڈیوائس سے دوسرے میں سفر کرتا ہے، چاہے وہ ایک کمرے کے اندر ہو یا دنیا بھر میں۔ ہر نیٹ ورک کی قسم ایک مخصوص مقصد کی خدمت کرتی ہے اور مختلف ریٹخ اور سائز کو سنبھالنے کے لیے

تیار کیا گیا ہے۔



شکل 6.19: CAN

6.11 کمپیوٹر نیٹ ورکس کی حقیقی دنیا کی اپیلی کیشنز

6.11.1 کاروبار

کاروبار میں، نیٹ ورک موثر کمیونیکیشن، وسائل کے اشتراک، اور ڈیٹا مینجمنٹ کے قابل بناتا ہے۔ مثال: کمپنیاں ادارے کے اندر معلومات اور وسائل کو محفوظ طریقے سے میسر کرنے کے لیے انٹرانٹ کا استعمال کرتی ہیں۔

6.11.1 تعلیم

تعلیمی ادارے آن لائن لرننگ پلیٹ فارم، ورچوئل کلاس رومز اور تعلیمی وسائل تک رسائی فراہم کرنے کے لیے نیٹ ورکس کا استعمال کرتے ہیں۔

مثال: یونیورسٹیاں کورس کے مواد اور تشخیص فراہم کرنے کے لیے ”بلیک بورڈ“ اور ”موڈی“ جیسے لرننگ مینجمنٹ سسٹم (LMS) کا استعمال کرتی ہیں۔

6.11.2 صحت کی دیکھ بھال

صحت کی دیکھ بھال کے نیٹ ورک مریضوں کی معلومات، ٹیلی میڈیسن، اور طبی ڈیٹا بیس تک رسائی کے اشتراک کی سہولت فراہم کرتے ہیں۔

مثال: ہسپتال مریضوں کے اعداد و شمار کو موثر طریقے سے ذخیرہ کرنے اور بازیافت کرنے کے لیے الیکٹرانک ہیلتھ ریکارڈ (EHR) سسٹم کا استعمال کرتے ہیں۔

6.12 TCP/IP کمیونیکیشن میں معیاری پروٹوکول

6.12.1 ٹرانسمیشن کنٹرول پروٹوکول / انٹرنیٹ پروٹوکول (TCP/IP) کا تعارف

انٹرنیٹ کمیونیکیشن کے لیے پروٹوکول کا بنیادی مجموعہ ہے۔

6.12.2 سینڈرڈ پروٹوکول

- (i) ٹرانسمیشن کنٹرول پروٹوکول (TCP) : قابل اعتماد ڈیٹا منتقلی کو یقینی بناتا ہے۔
- (ii) انٹرنیٹ پروٹوکول (IP) : ڈیٹا پیکیٹوں سے خطاب اور روٹنگ کو سنبھالتا ہے۔
- (iii) یوزر ڈیٹا گرام پروٹوکول (UDP) : تیز تر، لیکن کم قابل اعتماد، ڈیٹا ٹرانسفر فراہم کرتا ہے۔
- (iv) ڈومین نیم سسٹم (DNS) : ڈومین ناموں کو آئی پی پتوں میں ترجمہ کرتا ہے۔
- (v) ڈائنامک ہوسٹ کنفگریشن پروٹوکول (DHCP) : خود بخود آئی پی پتے تفویض کرتا ہے۔

6.13 نیٹ ورک سیکورٹی کے طریقے

6.13.1 فائر والز

آنے اور جانے والے نیٹ ورک ٹریفک کی نگرانی اور کنٹرول کریں۔

6.13.2 خفیہ کاری

ڈیٹا کو محفوظ فارمیٹ میں تبدیل کر کے اس کی حفاظت کرتا ہے۔

6.13.3 اینٹی وائرس سافٹ ویئر

بد نیقی پر مبنی سافٹ ویئر کا پتہ لگاتا ہے اور اسے ہٹاتا ہے۔

مثال: فائر والز، خفیہ کاری، اور اینٹی وائرس سافٹ ویئر کا مجموعہ مضبوط نیٹ ورک سیکورٹی فراہم کرتا ہے۔

سرگرمی

طلبہ کو مختلف نیٹ ورک سیکورٹی طریقوں کے فوائد اور نقصانات پر تبادلہ خیال کریں۔

خلاصہ

- ایک کمپیوٹر نیٹ ورک ایک دوسرے سے منسلک کمپیوٹرز اور آلات کا ایک نظام ہے جو وسائل کو کمیونیکیشن اور میسر کرتے ہیں۔
- کمپیوٹر نیٹ ورکس کے بنیادی مقاصد وسائل کے اشتراک، ڈیٹا مواصلات اور آلات کے درمیان رابطے کو قابل بنانا ہے۔
- ڈیٹا کمیونیکیشن میں پیغام رسانی کے ذریعے مرسل اور وصول کنندہ کے درمیان ڈیٹا کا تبادلہ شامل ہوتا ہے۔
- پروٹوکول قوانین کے سیٹ ہیں جو ڈیٹا کمیونیکیشن کو کنٹرول کرتے ہیں۔ عام پروٹوکول میں TCP/IP، HTTP، FTP اور SMTP شامل ہیں۔
- راؤٹر ایک ایسا آلہ ہے جو مختلف نیٹ ورکس کو ایک ساتھ جوڑتا ہے اور ان کے درمیان ڈیٹا پیکیٹوں کو ہدایت کرتا ہے۔
- جب آپ انٹرنیٹ پر ڈیٹا بھیجتے ہیں تو، یہ چھوٹے ٹکڑوں میں ٹوٹ جاتا ہے جسے پیکٹ کہا جاتا ہے۔
- سوچ ایک نیٹ ورک آلہ ہے جو مقامی علاقے کے نیٹ ورک (LAN) کے اندر متعدد آلات (جیسے کمپیوٹرز، پرنٹرز اور سرورز) کو

جوڑتا ہے۔

ایکسیس پوائنٹ (AP) ایک نیٹ ورک ڈیوائس ہے جو وائرلیس ڈیوائسز کو وائرڈ نیٹ ورک سے منسلک کرنے کی سہولت دیتا ہے۔

نیٹ ورک ٹپالوجی کمپیوٹر نیٹ ورک میں مختلف عناصر (لنکس، نوڈز، وغیرہ) کی ترتیب سے مراد ہیں۔

بس ٹپالوجی میں، تمام آلات ایک ہی مواصلاتی لائن کا اشتراک کرتے ہیں جسے بس کہا جاتا ہے۔ ہر آلہ اس مرکزی کیبل سے جڑا ہوا ہے۔

اسٹار ٹپالوجی میں، تمام آلات مرکزی مرکز یا سوئچ سے منسلک ہوتے ہیں۔ ہب ڈیٹا کے بہاؤ کے لیے ریپیٹر کے طور پر کام کرتا ہے۔

رنگ ٹپالوجی میں، ہر ڈیوائس کو دوسرے آلات سے منسلک کیا جاتا ہے، جس سے سرکلر ڈیٹا کا راستہ بنتا ہے۔ ڈیٹا ایک سمت میں سفر کرتا ہے، ہر آلے سے گزرتا ہے۔

میش ٹپالوجی میں، ہر آلہ ہر دوسرے آلے سے منسلک ہوتا ہے۔ یہ اعلیٰ اضافی اور قابل اعتماد فراہم کرتا ہے۔

سمپلکس کمیونیکیشن میں، ڈیٹا ٹرانسمیشن یک سمتی ہے، جس کا مطلب ہے کہ یہ صرف ایک سمت میں بہہ رہا ہے۔

ہاف ڈوپلکس کمیونیکیشن میں، ڈیٹا ٹرانسمیشن دونوں سمتوں میں ہو سکتی ہے، لیکن بیک وقت نہیں۔

فل ڈوپلکس کمیونیکیشن میں، ڈیٹا ٹرانسمیشن بیک وقت دونوں سمتوں میں ہو سکتی ہے۔

اوپن سسٹم انٹر کنکشن (OSI) ماڈل ایک فریم ورک ہے جو یہ سمجھنے کے لیے استعمال ہوتا ہے کہ مختلف نیٹ ورکنگ پروٹوکول کس طرح تعامل کرتے ہیں۔

انٹرنیٹ پروٹوکول (IP) ایڈریس انٹرنیٹ سے منسلک آلات کو تفویض کردہ منفرد شناخت کنندہ ہیں۔ اس کے دو بنیادی ورژن ہیں: IPv4 کو IPv6۔

DNS ڈومین ناموں کو IP ایڈریس پر ترجمہ کرتا ہے، جس سے صارفین کے لیے ویب سائٹس تک رسائی آسان ہو جاتی ہے۔

DHCP نیٹ ورک مینجمنٹ کو آسان بناتے ہوئے خود بخود نیٹ ورک پر موجود ڈیوائسز کو IP ایڈریس تفویض کرتا ہے۔

نیٹ ورک سکیورٹی میں ڈیٹا کی حفاظت اور کمپیوٹر نیٹ ورکس تک غیر مجاز رسائی کو روکنے کے اقدامات شامل ہیں۔

خفیہ کاری ڈیٹا کو ایک محفوظ شکل میں تبدیل کرتی ہے جسے صرف صحیح ڈیکریپشن کی ساتھ مجاز فریقوں کے ذریعہ پڑھایا سمجھا جاسکتا ہے۔

PAN ایک چھوٹا سائٹ ورک ہے جو مختصر رینج کے اندر ذاتی آلات، جیسے اسمارٹ فونز، ٹیبلیٹس اور لیپ ٹاپ کے مابین کمیونیکیشن کے لیے استعمال ہوتا ہے۔

LAN ایک ایسا نیٹ ورک ہے جو کمپیوٹرز اور آلات کو ایک محدود علاقے کے اندر جوڑتا ہے، جیسے گھر، اسکول، یا دفتر کی عمارت۔

MAN ایک ایسا نیٹ ورک ہے جو ایک شہر یا بڑے کمپس تک پھیلا ہوا ہے، جو متعدد LANs کو ایک ساتھ جوڑتا ہے۔

- ایک WAN ایک بڑے جغرافیائی علاقے کا احاطہ کرتا ہے، جو متعدد LANs اور MANs کو جوڑتا ہے۔ انٹرنیٹ WAN کی سب سے بڑی مثال ہے۔
- CAN ایک ایسا نیٹ ورک ہے جو ایک محدود جغرافیائی علاقے کے اندر متعدد LANs کو جوڑتا ہے، جیسے یونیورسٹی کمپیوٹس یا کاروبار۔

مشق

1۔ درست جواب کا انتخاب کریں:

- (i) کمپیوٹر نیٹ ورکس کا بنیادی مقصد کیا ہے؟
 (الف) کمپیوٹیشنل طاقت میں اضافہ
 (ج) گرافکس کی صلاحیتوں میں اضافہ
 (ii) کون سا آلہ متعدد نیٹ ورکس کو جوڑنے اور ان کے درمیان ڈیٹا پیکیٹس کی رہنمائی کے لیے استعمال ہوتا ہے؟
 (الف) سوئیچ
 (ج) روٹر
 (iii) OSI ماڈل کی کون سی لیئر Node-to-Node ڈیٹا ٹرانسفر اور غلطیوں کی نشاندہی کے لیے ذمہ دار ہے؟
 (الف) فزیکل لیئر
 (ج) نیٹ ورک لیئر
 (iv) ڈومین نیم سسٹم (DNS) کا کیا کام ہے؟
 (الف) آئی پی ایڈریسز کو متحرک طور پر تفویض کرنا
 (ج) ڈیٹا کی کمیونیکیشن کو محفوظ بنانا
 (v) ڈیٹا کی ترسیل کا کون سا طریقہ ایک مخصوص مواصلاتی راستہ استعمال کرتا ہے؟
 (الف) پیکٹ سوئیچنگ
 (ج) سرکٹ سوئیچنگ
 (vi) نیٹ ورک کمیونیکیشن کے سیاق و سباق میں انکسپولیشن کیا ہے؟
 (الف) ڈیٹا کو ایک محفوظ شکل میں تبدیل کرنا
 (ج) نیٹ ورک ٹریفک کی نگرانی کرنا
 (ب) وسائل کی شراکت اور ڈیٹا کی ترسیل کو ممکن بنانا
 (د) سافٹ ویئر ڈیولپمنٹ کو بہتر بنانا
 (ب) ڈیٹا لنک لیئر
 (د) ٹرانسپورٹ لیئر
 (ب) ڈومین ناموں کو آئی پی ایڈریسز میں ترجمہ کرنا
 (د) نیٹ ورک ٹریفک کی نگرانی کرنا
 (ب) پروٹوکول معلومات کے ساتھ ڈیٹا کو لپیٹنا
 (د) ڈومین ناموں کو آئی پی ایڈریسز میں ترجمہ کرنا

(vii) TCP/IP ماڈل میں ڈیٹا کی قابل اعتماد ترسیل کے لیے کون سا پروٹوکول استعمال ہوتا ہے؟

FTP (ب)

HTTP (الف)

UDP (د)

TCP (ج)

(viii) نیٹ ورک سیکیورٹی میں فائر وال کا بنیادی مقصد کیا ہے؟

(الف) ڈیٹا کو ایک محفوظ شکل میں تبدیل کرنا

(ب) نیٹ ورک ٹریفک کی نگرانی اور کنٹرول کرنا

(د) ڈومین ناموں کا ترجمہ کرنا

(ج) آئی پی ایڈریسز تفویض کرنا

(ix) کون سی نیٹ ورک ٹپالوجی تمام ڈیوائسز کو ایک مرکزی حب سے جوڑتی ہے؟

(ب) میس

(الف) رنگ

(د) اسٹار

(ج) بس

(x) کاروبار میں کمپیوٹر نیٹ ورکس کے استعمال کا ایک اہم فائدہ کیا ہے؟

(ب) وسائل کی شراکت اور موثر کمیونیکیشن کو ممکن بنانا

(الف) کمپیوٹر نیٹ ورکس میں اضافہ

(د) سافٹ ویئر ڈیولپمنٹ کو بہتر بنانا

(ج) گرافکس کی صلاحیتوں کو بہتر بنانا

2- مختصر سوالات

(i) ڈیٹا کمیونیکیشن کی وضاحت کریں اور اس کے اہم اجزاء کی فہرست بنائیں۔

(ii) کمپیوٹر نیٹ ورک میں روٹرز کے کردار کی وضاحت کریں۔

(iii) OSI ماڈل میں نیٹ ورک لیئر کے اہم افعال کیا ہیں؟

(iv) پیکٹ سوچنگ اور سرکٹ سوچنگ کے درمیان فرق کی وضاحت کریں۔

(v) DHCP کا مقصد کیا ہے؟

(vi) Encapsulation نیٹ ورک میں محفوظ کمیونیکیشن کو کیسے یقینی بناتا ہے؟

(vii) ڈیٹا ٹرانسفر قابل اعتماد کے لحاظ سے TCP اور UDP کے درمیان فرق کریں۔

(viii) نیٹ ورک سیکیورٹی میں خفیہ کاری کی اہمیت کی وضاحت کریں۔

(ix) نیٹ ورک میں اسٹار ٹپالوجی استعمال کرنے کے فوائد کیا ہیں؟

(x) فائر والز نیٹ ورک کی حفاظت میں کس طرح کردار ادا کرتے ہیں؟

3- تفصیلی سوالات

(i) کمپیوٹر نیٹ ورکس کے مقاصد پر تبادلہ خیال کریں اور مثالیں فراہم کریں کہ وہ وسائل کے اشتراک اور ڈیٹا کمیونیکیشن کی سہولت کیسے فراہم کرتے ہیں۔

- (ii) سمپلیکس کمیونیکیشن میں فرض کریں کہ ڈیٹا 500 بٹس فی سیکنڈ (BPS) کی شرح سے منتقل ہوتا ہے۔ پیغام منتقل کرنے کے لیے وقت کا حساب کریں اگر:
- (الف) یہ 10 کلوبائٹس کا ہے۔ (ب) یہ 10 کلوبائٹس کا ہوتا ہے۔
- (iii) پیکٹ سوچنگ اور سرکٹ سوچنگ کا استعمال کرتے ہوئے کمپیوٹر نیٹ ورکس میں ڈیٹا کیسے منتقل ہوتا ہے اس کی وضاحت کریں۔
- (iv) ڈیٹا کمیونیکیشن میں پروٹوکول کے کردار اور اہمیت پر تبادلہ خیال کریں۔ اہم پروٹوکول جیسے DNS، TCP/IP، HTTP اور DHCP کے افعال کی وضاحت کریں۔
- (v) نیٹ ورک کی حفاظت کے مختلف طریقوں کا جائزہ لیں، بشمول فائر والز، خفیہ کاری، اور اینٹی وائرس سافٹ ویئر۔
- (vi) کاروبار، تعلیم، اور صحت کی دیکھ بھال میں کمپیوٹر نیٹ ورکس کی حقیقی دنیا کی اپیلی کیشنز کی وضاحت کریں۔
- (vii) مختلف قسم کے نیٹ ورک ٹپالوجیز (Star, Ring, Bus and Mesh) کا موازنہ اور تقابل کریں۔
- (viii) 4 کی شفٹ کی مقدار کے ساتھ شفٹ سائفر پر غور کریں۔
- (الف) پیغام "Security" کو خفیہ کریں۔
- (ب) پیغام "WMXYVMI" کو ڈیکرپٹ کریں۔
- (ix) ایک IPv4 ایڈریس ایک 32 بٹ نمبر ہے۔ منفرد IPv4 ایڈریسز کی کل تعداد کا حساب لگائیں۔
- (الف) IPv4 ایڈریسز کی کل تعداد کا حساب دکھائیں۔
- (ب) اگر کل ایڈریسز کا 10% خصوصی مقاصد کے لیے محفوظ ہے تو کتنے ایڈریسز باقی رہ جاتے ہیں؟