इलेक्ट्रॉनिक्स और हार्डवेयर
Electronics & Hardware

सहायक पुस्तिका   कक्षा 12   2025-26

राज्य शैक्षिक अनुसंधान एवं प्रशिक्षण परिषद

वरुण मार्ग, डिफेंस कॉलोनी, नई दिल्ली - 110025

इलेक्ट्रॉनिक्स और हार्डवेयर

ELECTRONICS & HARDWARE

(Subject Code: 847)

SCERT DELHI

Class XII (2025-26)

SCERT
स्वाध्यायान्मा प्रमदः

State Council of Educational Research & Training, Delhi
varun Marg, Defence Colony, New Delhi - 110024

ISBN: 978-93-6291-937-3
© राज्य शैक्षिक अनुसंधान एवं प्रशिक्षण परिषद, दिल्ली
अप्रैल, 2025

मुख्य सलाहकार

डॉ. रीता शर्मा, निदेशक, राज्य शैक्षिक अनुसंधान एवं प्रशिक्षण परिषद् , दिल्ली
डॉ. नाहर सिंह, संयुक्त निदेशक (शैक्षणिक), राज्य शैक्षिक अनुसंधान एवं प्रशिक्षण परिषद् , दिल्ली

सलाहकार

श्रीमती बिमला कुमारी, डी.डी.ई, वोकेशनल शिक्षा, दिल्ली
श्री राकेश बल, ओ.एस.डी, वोकेशनल ब्रांच, दिल्ली
श्री संजीव कुमार गौड़, ओ.एस.डी, वोकेशनल ब्रांच, दिल्ली

नोडल अधिकारी

श्रीमती रमन अरोड़ा,सहायक प्रोफेसर, राज्य शैक्षिक अनुसंधान एवं प्रशिक्षण परिषद् , दिल्ली
डॉ. अप्सरा अंसारी, सहायक प्रोफेसर, राज्य शैक्षिक अनुसंधान एवं प्रशिक्षण परिषद् , दिल्ली

विषय समन्वयक

डॉ. भारतेन्दु गुप्ता, सहायक प्रोफेसर, मंडलीय शिक्षा एवं प्रशिक्षण संस्थान, भोला नाथ नगर, दिल्ली
डॉ. सुनील कुमार, सहायक प्रोफेसर, मंडलीय शिक्षा एवं प्रशिक्षण संस्थान, भोला नाथ नगर, दिल्ली
डॉ. शिनम बत्रा, सहायक प्रोफेसर, मंडलीय शिक्षा एवं प्रशिक्षण संस्थान, भोला नाथ नगर, दिल्ली

लेखक एवं समीक्षक समूह

डॉ. अनिल कुमार तेवतिया, प्राचार्य, मंडलीय शिक्षा एवं प्रशिक्षण संस्थान, भोला नाथ नगर, दिल्ली
डॉ. भारतेन्दु गुप्ता, सहायक प्रोफेसर, मंडलीय शिक्षा एवं प्रशिक्षण संस्थान, भोला नाथ नगर, दिल्ली
डॉ. सुनील कुमार, सहायक प्रोफेसर, मंडलीय शिक्षा एवं प्रशिक्षण संस्थान, भोला नाथ नगर, दिल्ली
डॉ. शिनम बत्रा, सहायक प्रोफेसर, मंडलीय शिक्षा एवं प्रशिक्षण संस्थान, भोला नाथ नगर, दिल्ली
डॉ. नीरा साध, सहायक प्रोफेसर, मंडलीय शिक्षा एवं प्रशिक्षण संस्थान, भोला नाथ नगर, दिल्ली
श्री संजीव कुमार गौड़, ओ.एस.डी, वोकेशनल ब्रांच, दिल्ली
मो. इमरान, जी.बी.एस.एस.एस. (द्वितीय शिफ्ट) नारायणा, दिल्ली
श्री अजय कुमार, जी.बी.एस.एस.एस., टैंक रोड देव नगर, दिल्ली
मोहम्मद तबरेज़ खान, जी.बी.एस.एस.एस., नंबर-3, मोलर बंद, दिल्ली
श्री दीपक कुमार, जी.बी.एस.एस.एस. नंबर-2, डीडीए फ्लैट्स बदरपुर, दिल्ली
श्रीमती यामीका साध, अटल आदर्श बालिका सीनियर सेकेंडरी विद्यालय, गोल मार्किट, दिल्ली

प्रकाशन अधिकारी

डॉ. मुकेश यादव,राज्य शैक्षिक अनुसंधान एवं प्रशिक्षण परिषद्, दिल्ली

प्रकाशन दल

श्री दिनेश कुमार शर्मा, (ए.एस.ओ.), राज्य शैक्षिक अनुसंधान एवं प्रशिक्षण परिषद्, दिल्ली
सुश्री फ़ौजिया, (बी.आर.पी.), राज्य शैक्षिक अनुसंधान एवं प्रशिक्षण परिषद्, दिल्ली

प्रकाशित : राज्य शैक्षिक अनुसंधान एवं प्रशिक्षण परिषद, नई दिल्ली

मुद्रित : राज प्रिंटर्स, ए-9, सेक्टर बी-2, ट्रोनिका सिटी, लोनी, गाज़ियाबाद (यू.पी.)

Dr. Rita Sharma
Director SCERT

SCERT
स्वाध्यायान्मा प्रमदः

STATE COUNCIL OF EDUCATIONAL RESEARCH and TRAINING
(An autonomous Organisation of GNCT of Delhi)
Varun Marg, Defence Colony, New Delhi-110024
Tel.: +91-11-24331356
E-mail : dir12scert@gmail.com

Date : 29/5/2025

D.O. No. : F.1.0(1)/DPB/AH Conv/37

संदेश

"राष्ट्रीय शिक्षा नीति 2020" के अंतर्गत स्कूली शिक्षा में व्यावसायिक शिक्षा के एकीकरण पर विशेष बल दिया गया है, जिससे विद्यार्थियों को प्रारंभिक स्तर से ही जीवनोपयोगी और रोजगारोन्मुख कौशलों से जोड़ा जा सके। यह नीति ज्ञान और कौशल के समन्वय से आत्मनिर्भर भारत के निर्माण की दिशा में एक महत्वपूर्ण पहल है।

इसी उद्देश्य की पूर्ति हेतु राज्य शैक्षिक अनुसंधान एवं प्रशिक्षण परिषद (SCERT), दिल्ली द्वारा वरिष्ठ माध्यमिक स्तर के विद्यार्थियों के लिए विभिन्न व्यावसायिक विषयों जैसे कि **ऑटोमोटिव, सौंदर्य एवं कल्याण, इलेक्ट्रॉनिक्स और हार्डवेयर, रोज़गार कौशल, वित्तीय बाज़ार प्रबंधन, सूचना प्रौद्योगिकी, खाद्य उत्पाद, स्वास्थ्य देखभाल, विपणन, शारीरिक गतिविधि प्रशिक्षक, रिटेल/खुदरा तथा पर्यटन** के लिए सहायक सामग्री का निर्माण किया गया है।

इन विषयों की सहायक सामग्री इस प्रकार तैयार की गई है कि वह विद्यार्थियों को विषय की मूल अवधारणाओं को समझने, व्यावहारिक रूप से लागू करने और 21वीं सदी के आवश्यक कौशल विकसित करने में सहायता करे। इसमें शिक्षकों के लिए उपयोगी शिक्षण विधियाँ, गतिविधियाँ, मूल्यांकन सुझाव और केस स्टडी जैसे घटकों को शामिल किया गया है, जो शिक्षण को अधिक प्रभावशाली और रोचक बनाते हैं।

आशा है कि यह सहायक सामग्री शिक्षकों एवं विद्यार्थियों के लिए उपयोगी सिद्ध होगी।

रीता शर्मा

(डॉ. रीता शर्मा)
निदेशक

SCERT
स्वाध्यायान्मा प्रमदः

Dr. Nahar Singh
Joint Director (Academic)

State Council of Educational Research and Training
(An autonomous Organisation of GNCT of Delhi)
Tel. : +91-11-24336818, 24331355, Fax : +91-11-24332426
Tel.: +91-11-24331355, Fax : +91-11-24332426
E-mail : jdscertdelhi@gmail.com

Date : 26/05/2025

D.O. No. : F.11(2)JDB/Acad/Misc/SCERT/2025-26/404

संदेश

व्यावसायिक शिक्षा वर्तमान युग की एक अनिवार्य आवश्यकता बन चुकी है, जो विद्यार्थियों को न केवल शैक्षणिक ज्ञान देती है, बल्कि उन्हें व्यावहारिक कौशल और आत्मनिर्भरता की दिशा में भी अग्रसर करती है। **राष्ट्रीय शिक्षा नीति 2020** इसी सोच को साकार करने का एक सशक्त माध्यम है, जो शिक्षा को समग्रता प्रदान करती है।

राज्य शैक्षिक अनुसंधान एवं प्रशिक्षण परिषद, दिल्ली द्वारा व्यावसायिक विषयों के लिए तैयार की गई यह **सहायक सामग्री** शिक्षकों और विद्यार्थियों दोनों के लिए उपयोगी संसाधन है। इसमें पाठ्यवस्तु को सरल और रोचक तरीके से प्रस्तुत किया गया है, जिससे विद्यार्थियों को विषयों की गहरी समझ विकसित करने में सहायता मिलेगी। यह सामग्री न केवल सीखने की प्रक्रिया को प्रभावी बनाएगी, बल्कि छात्रों में आत्मविश्वास और कौशल विकसित करने की दृष्टि से भी महत्वपूर्ण सिद्ध होगी।

यह सामग्री विद्यार्थियों और शिक्षकों के लिए एक दिशा-निर्देशक की तरह कार्य करेगी, जिससे वे विषय को वास्तविक जीवन से जुड़ा हुआ एवं अनुभव आधारित बना सके।

(डॉ. नाहर सिंह)
संयुक्त निदेशक

प्रस्तावना

प्रस्तुत सहायक सामग्री (support material) इलेक्ट्रानिक्स और हार्डवेयर (Electronics and Hardware) NSQF के नवीनतम् पाठ्यक्रमानुसार कक्षा -12 के लिए तैयार किया गया है, सामान्यतः विद्यार्थियों को कुछ मूल शब्दों का अर्थ समझने में कठिनाइयों का सामना करना पड़ता है। इसीलिये विद्यार्थियों की प्रत्येक समस्याओं को ध्यान में रखते हुए हिंदी में सहायक सामग्री का निर्माण किया गया है। सहायक सामग्री में प्रयुक्त मूल शब्दों को हिंदी तथा अंग्रेजी दोनों भाषाओं में प्रस्तुत किया गया है। सहायक सामग्री की भाषा को अत्यंत सरल एवं प्रभावशाली रखा गया है ताकि विद्यार्थियों को पढ़ने और समझने में असुविधा का सामना न करना पड़े। पाठ के अंत में अभ्यास प्रश्न (Exercises) दिए गए हैं ताकि विद्यार्थी अपना मूल्यांकन स्वयं कर सकें। इनमें बहुविकल्पीय प्रश्न (Multiple Choice Questions), संक्षिप्त प्रश्न (Short Answer Questions) सम्मिलित हैं। सहायक सामग्री में पर्याप्त चित्रों का समावेश किया गया है जिससे पुस्तक पढ़ने में विद्यार्थियों की रुचि बनी रहती है।

SCERT DELHI

परिचय

विंडोज सर्वर की स्थापना और कॉन्फ़िगरेशन सरल प्रक्रिया है जिसमें ऑपरेटिंग सिस्टम की स्थापना, डोमेन कंट्रोलर सेटअप, और आवश्यक सेवाओं को कॉन्फ़िगर करना शामिल है। लिनक्स सर्वर में टर्मिनल कमांड का उपयोग कर स्थापना होती है, जो विभिन्न वितरणों (डिस्ट्रो) के लिए अलग-अलग होती है। आईटी सुरक्षा के बुनियादी सिद्धांतों में डेटा एन्क्रिप्शन, फ़ायरवॉल, एंटीवायरस सॉफ़्टवेयर का उपयोग और नेटवर्क सुरक्षा शामिल है। यह सिद्धांत सुनिश्चित करते हैं कि डेटा और सिस्टम सुरक्षित रहें। दोनों सर्वर और सुरक्षा प्रक्रियाओं की सही स्थापना से नेटवर्क और डेटा की सुरक्षा बढ़ाई जा सकती है। आईटीआईएल v3 आईटी सेवा प्रबंधन के लिए एक रूपरेखा है, जो सेवाओं की योजना, वितरण, संचालन और सुधार पर केंद्रित है, ताकि व्यवसाय की ज़रूरतों को प्रभावी ढंग से पूरा किया जा सके।

SCERT DELHI

विषय सूची

इकाई	विवरण	पृष्ठ संख्या
1.	**कंप्यूटर नेटवर्क की आवश्यकताएँ**	1-15
	नेटवर्किंग का विकास	2
	नेटवर्क के प्रकार	3
	नेटवर्क डिवाइस	5
	नेटवर्क टोपोलॉजी	7
	ओपन सिस्टम इंटरकनेक्शन मॉडल	9
	नेटवर्क तकनीकें	11
	डेटा ट्रांसमिशन	12
2.	**विंडोज सर्वर की स्थापना और कॉन्फ़िगरेशन**	16-44
	Regular Windows और Windows Server में अंतर	16
	Windows Server 2012 की इंस्टॉलेशन का स्टेप-बाय-स्टेप प्रोसेस	17
	Windows Server पर पोस्ट-इंस्टॉलेशन कार्य	20
	Windows Server 2012 को प्रबंधित करना	24
	A.D.D.S को इंस्टॉल और कॉन्फिगर करना	26
	डोमेन कंट्रोलर्स (Domain Controllers) का अवलोकन	27
	डोमेन कंट्रोलर इंस्टॉल करना	28
	Active Directory Domain की संरचना (Structure)	32
	Windows PowerShell का उपयोग करके यूज़र अकाउंट बनाना	38
	यूज़र अकाउंट को डिलीट करने का तरीका	40
3.	**लिनक्स सर्वर की स्थापना और कॉन्फ़िगरेशन**	45-60
	लिनक्स सर्वर की स्थापना प्रक्रिया	46
	लिनक्स सर्वर प्रबंधन का अवलोकन	49

इकाई	विवरण	पृष्ठ संख्या
	लिनक्स सर्वर प्रबंधन की प्रक्रिया	50
	लिनक्स की फ़ाइल संरचना	52
	लिनक्स फ़ाइल संरचना के प्रकार	54
	सेवाओं के लिए पैकेज इंस्टॉल करना और हटाना	56
4.	**आईटी सुरक्षा के बुनियादी सिद्धांत**	61-75
	आईटी सुरक्षा के सिद्धांत	61
	एंटीवायरस सॉफ्टवेयर का उपयोग	63
	एंटीवायरस सॉफ्टवेयर का उपयोग कैसे करें	64
	कमज़ोरियों (Vulnerabilities) का वर्णन	65
	सुरक्षा प्रक्रियाएँ (Security Procedures)	66
	सुरक्षित डेटा (Protected Data) का वर्णन	68
	फायरवॉल के उपयोग	70
	एप्लिकेशन लेवल गेटवे प्रॉक्सी फायरवॉल	71
5.	**आईटीआईएल v3 की मूल बातें**	**76-90**
	आईटीआईएल की आवश्यकता	76
	आईटीआईएल के संस्करण	78
	आईटीआईएल प्रकाशन	80
	आईटीआईएल के लाभ	81
	आईटीआईएल v2 बनाम आईटीआईएल v3 (ITIL v2 vs ITIL v3)	83
	सेवा (Service) की अवधारणाएँ	85
	आईटी सेवा प्रबंधन	85
	समस्या प्रबंधन	88

कंप्यूटर नेटवर्क की आवश्यकताएँ

अध्याय 1

परिचय

कंप्यूटर नेटवर्क एक ऐसा संग्रह है जिसमें जुड़े हुए उपकरण एक- दूसरे के साथ संवाद करते हैं ताकि संसाधनों और जानकारी को साझा किया जा सके। यह आधुनिक कंप्यूटिंग और संचार में महत्वपूर्ण हैं, जो उपयोगकर्ताओं को विभिन्न भौगोलिक स्थानों पर डेटा अनुप्रयोग और सेवाओं तक पहुँचने में सक्षम बनाते हैं।

नेटवर्क के प्रकार:

* **लोकल एरिया नेटवर्क (LAN):** एक छोटे भौगोलिक क्षेत्र, जैसे घर, कार्यालय या परिसर में फैला होता है।
* **वाइड एरिया नेटवर्क (WAN):** बड़े भौगोलिक क्षेत्र को कवर करता है, अक्सर कई LANs को जोड़ता है; इंटरनेट सबसे बड़ा WAN है।
* **मेट्रोपोलिटन एरिया नेटवर्क (MAN):** LAN से बड़ा लेकिन WAN से छोटा, आमतौर पर एक शहर या बड़े परिसर को कवर करता है।
* **पर्सनल एरिया नेटवर्क (PAN):** एक छोटे नेटवर्क, आमतौर पर कुछ मीटर की सीमा में, जैसे व्यक्तिगत उपकरणों (जैसे, ब्लूटूथ) को जोड़ना।

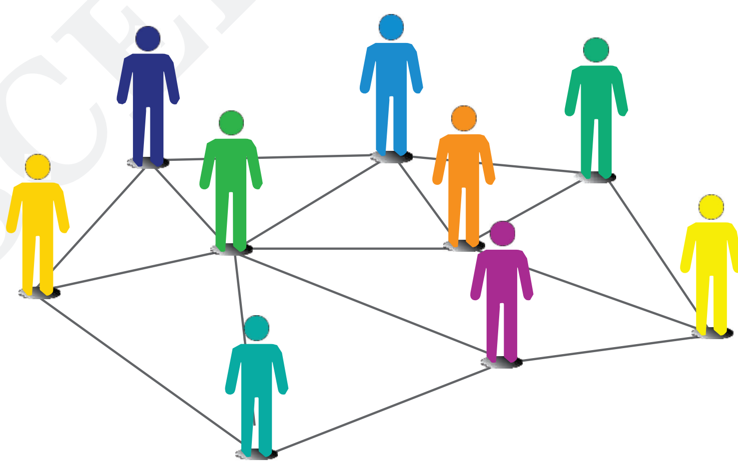


Figure 1.1: Interconnection forming a social network

SCERT DELHI

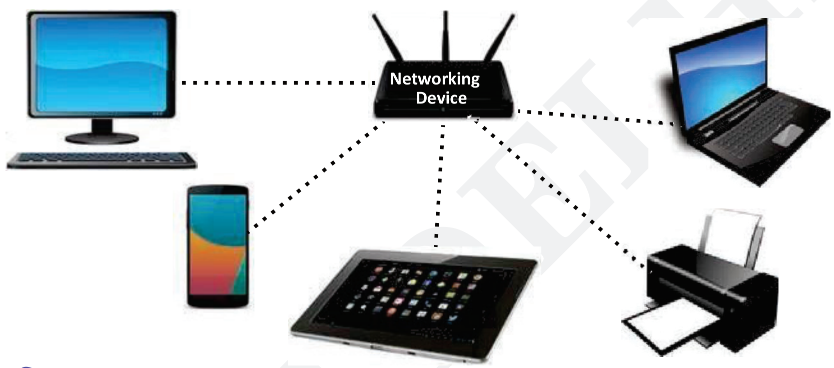
मुख्य अवधारणाएँ:

1. परिभाषा:

एक कंप्यूटर नेटवर्क हार्डवेयर (जैसे कंप्यूटर, राउटर, स्विच) और सॉफ़्टवेयर (प्रोटोकॉल और अनुप्रयोग) का संग्रह होता है, जो उपकरणों के बीच संवाद को सुविधाजनक बनाने के लिए एक साथ काम करते हैं।

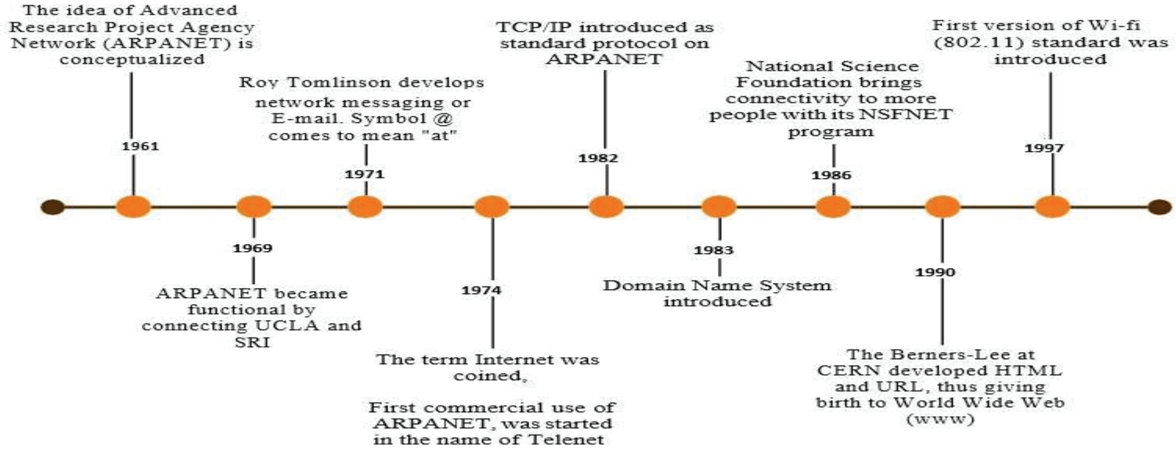
2. उद्देश्य:

संसाधन साझा करना कई उपयोगकर्ताओं को प्रिंटर, फ़ाइलों और इंटरनेट कनेक्शन जैसे संसाधनों को साझा करने की अनुमति देता है



1.2 नेटवर्किंग का विकास

नेटवर्किंग का विकास समय के साथ विभिन्न चरणों में हुआ है। प्रारंभ में, टेलीग्राफ और टेलीफोन जैसी पारंपरिक संचार तकनीकों का उपयोग किया गया। 1960 के दशक में ARPANET के माध्यम से पहला कंप्यूटर नेटवर्क स्थापित हुआ, जिसके बाद TCP/IP प्रोटोकॉल ने विभिन्न नेटवर्कों को जोड़ने में मदद की। 1980 के दशक में इंटरनेट का उदय हुआ, और 1990 के दशक में वेब ब्राउज़र ने इसे आम जनता के लिए सुलभ बना दिया। इसके बाद, वाई-फाई और मोबाइल नेटवर्किंग जैसे वायरलेस तकनीकों का विकास हुआ। 2000 के दशक में क्लाउड कंप्यूटिंग और इंटरनेट ऑफ थिंग्स (IoT) ने नेटवर्किंग को और भी विकसित किया। वर्तमान में, कृत्रिम बुद्धिमत्ता और साइबर सुरक्षा का ध्यान नेटवर्किंग के भविष्य को आकार दे रहा है।



1.3 नेटवर्क के प्रकार

नेटवर्क के विभिन्न प्रकार होते हैं, जो उनकी संरचना, कार्यक्षमता और उपयोग के आधार पर वर्गीकृत किए जा सकते हैं। प्रमुख नेटवर्क प्रकार निम्नलिखित हैं:

1. स्थानीय क्षेत्र नेटवर्क (LAN)

परिभाषा: LAN एक सीमित भौगोलिक क्षेत्र, जैसे कार्यालय या स्कूल के भीतर स्थापित होता है।

विशेषताएँ: तेज़ डेटा ट्रांसफर गति और कम लागत। आमतौर पर ईथरनेट या वाई-फाई का उपयोग करता है।

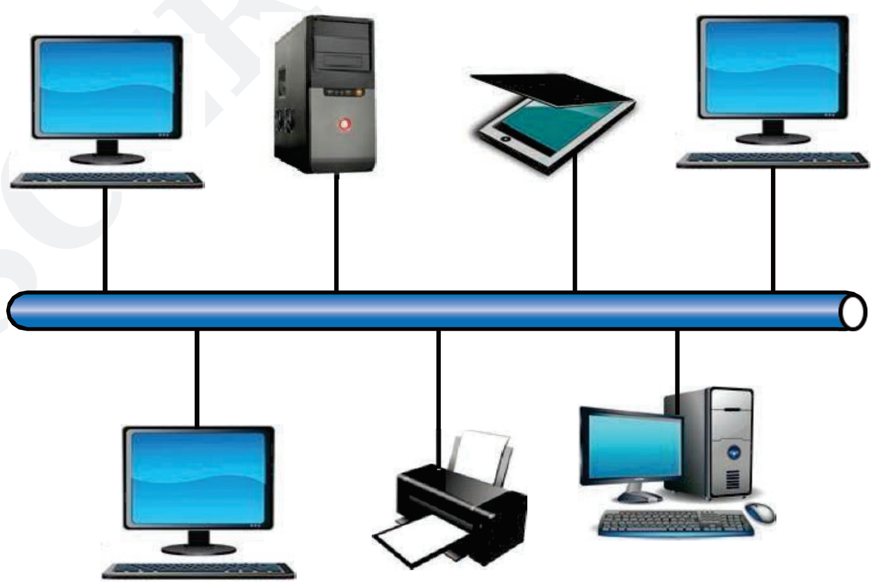


Figure 1.5: A Local Area Network

2. वाइड क्षेत्र नेटवर्क (WAN)

परिभाषा: WAN बड़े भौगोलिक क्षेत्रों, जैसे देशों या महाद्वीपों के बीच स्थापित होता है।

विशेषताएँ: इंटरनेट इसका सबसे बड़ा उदाहरण है। यह उच्च डेटा ट्रांसफर गति प्रदान करता है, लेकिन लागत अधिक हो सकती है।

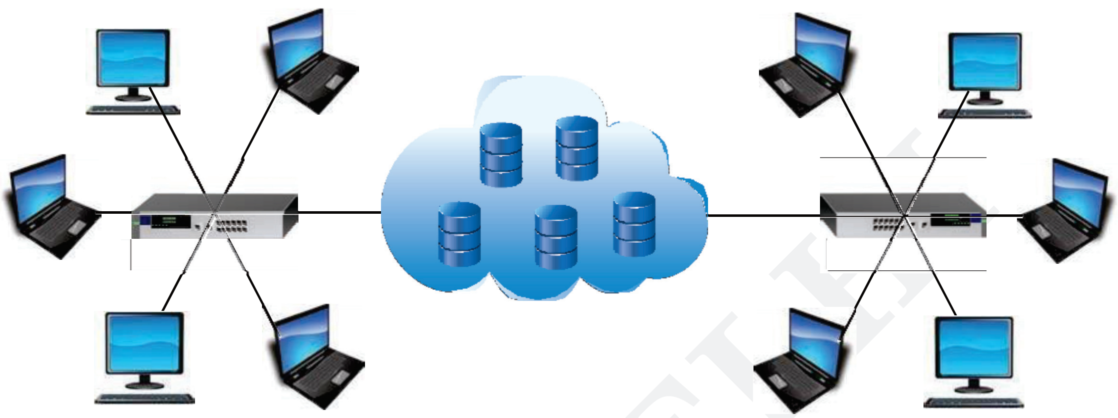


Figure 1.7: A Wide Area Network

3. मेट्रोपॉलिटन एरिया नेटवर्क (MAN)

परिभाषा: MAN एक शहर या बड़े क्षेत्र के भीतर नेटवर्क स्थापित करता है।

विशेषताएँ: LAN और WAN के बीच का क्षेत्र, यह आमतौर पर इंटरनेट सेवा प्रदाताओं द्वारा उपयोग किया जाता है।

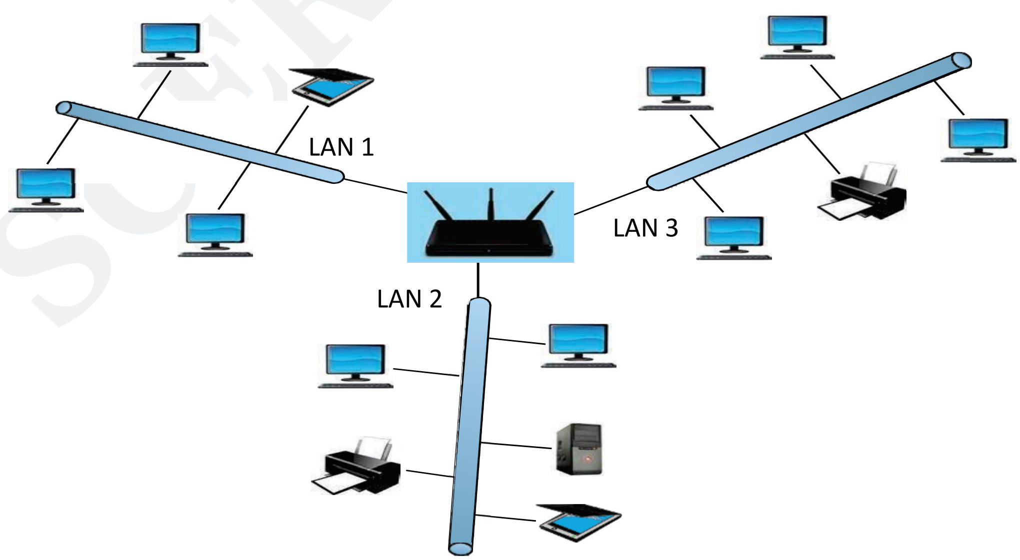


Figure 1.6: A Metropolitan Area Network

4. पर्सनल एरिया नेटवर्क (PAN)

परिभाषाः PAN छोटे क्षेत्र में, जैसे एक व्यक्ति के उपकरणों के बीच स्थापित होता है।

विशेषताएँः Bluetooth और USB कनेक्शन इसका उदाहरण हैं। यह व्यक्तिगत उपकरणों को जोड़ने के लिए प्रयोग होता है।

5. वर्चुअल प्राइवेट नेटवर्क (vPN)

परिभाषाः vPN एक सुरक्षित नेटवर्क है जो सार्वजनिक नेटवर्क पर डेटा को सुरक्षित रूप से संचारित करता है।

विशेषताएँः यह एन्क्रिप्शन का उपयोग करता है और आमतौर पर दूरस्थ कार्यकर्ताओं के लिए उपयोगी होता है।

1.4 नेटवर्क डिवाइस

नेटवर्क डिवाइस (Network Devices) ऐसे उपकरण होते हैं जो कंप्यूटर नेटवर्क में डेटा के संचार और प्रबंधन में मदद करते हैं। यहाँ कुछ प्रमुख नेटवर्क डिवाइस के बारे में जानकारी दी गई हैः

1. राउटर (Router):

* यह विभिन्न नेटवर्क को जोड़ने का काम करता है। राउटर डेटा पैकेट्स को एक नेटवर्क से दूसरे नेटवर्क में भेजता है।

स्विच (Switch):

यह एक लोकल एरिया नेटवर्क (LAN) में कई डिवाइस को जोड़ने के लिए उपयोग किया जाता है। स्विच डेटा को एक डिवाइस से दूसरे डिवाइस तक भेजता है।

हब (Hub):

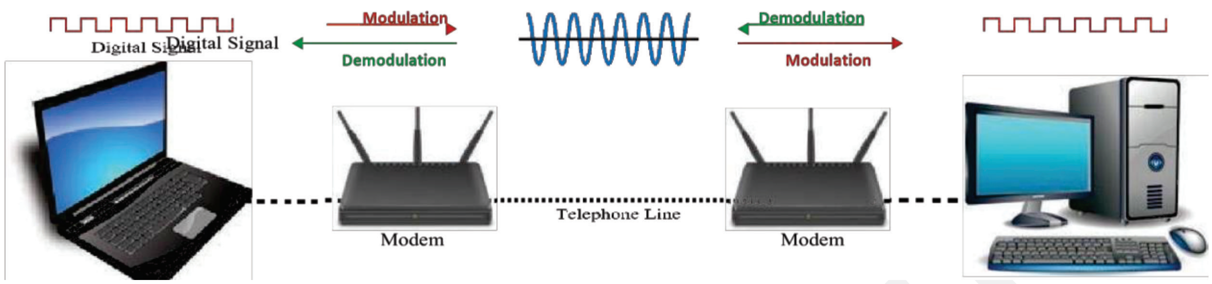
यह एक साधारण नेटवर्क डिवाइस है जो कई डिवाइस को जोड़ता है, लेकिन यह डेटा को सभी पोर्ट्स पर भेजता है, जिससे नेटवर्क ट्रैफिक बढ़ता है।

एक्सेस पॉइंट (Access Point):

यह वायरलेस डिवाइस है जो वाई-फाई नेटवर्क को स्थापित और प्रबंधित करता है, जिससे मोबाइल डिवाइस और लैपटॉप बिना तार के नेटवर्क से जुड़े रहते हैं।

मोडेम (Modem):

यह डिवाइस डिजिटल सिग्नल को एनालॉग सिग्नल में परिवर्तित करता है और इसके विपरीत, जिससे इंटरनेट कनेक्शन स्थापित होता है।



फायरवॉल (Firewall):

यह नेटवर्क की सुरक्षा के लिए प्रयोग किया जाता है। फायरवॉल नेटवर्क में आने-जाने वाले ट्रैफिक को नियंत्रित करता है और संभावित खतरों से सुरक्षा प्रदान करता है।

1.5 नेटवर्किंग टोपोलॉजी

नेटवर्क टोपोलॉजी (Networking Topologies) नेटवर्क के संरचनात्मक डिज़ाइन को दर्शाती है, जिसमें यह बताया जाता है कि नेटवर्क में डिवाइस एक-दूसरे से कैसे जुड़े हैं। यहाँ कुछ प्रमुख नेटवर्क टोपोलॉजी के प्रकार दिए गए हैं:

1. स्टार टोपोलॉजी (Star Topology):

* इस प्रकार में सभी डिवाइस एक केंद्रीय हब या स्विच से जुड़े होते हैं। डेटा सभी डिवाइसों के बीच इस हब के माध्यम से यात्रा करता है। यदि एक डिवाइस खराब हो जाता है, तो अन्य डिवाइस प्रभावित नहीं होते।

2. बस टोपोलॉजी (Bus Topology):

इसमें सभी डिवाइस एकल केबल (बस) पर जुड़े होते हैं। डेटा सभी डिवाइसों को एक ही केबल के माध्यम से भेजा जाता है। यदि केबल में कोई समस्या आती है, तो संपूर्ण नेटवर्क प्रभावित हो सकता है।

SCERT DELHI

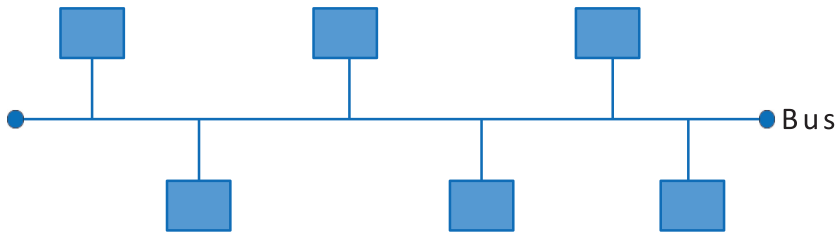
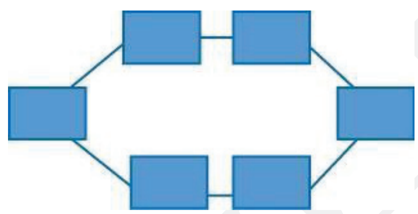


Figure 1.17: A bus topology

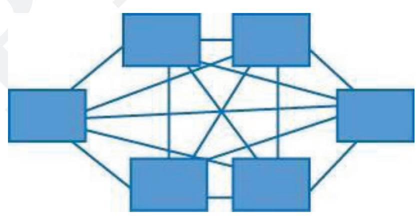
3. रिंग टोपोलॉजी (Ring Topology):

इसमें सभी डिवाइस एक-दूसरे से एक रिंग के रूप में जुड़े होते हैं। डेटा एक दिशा में चलता है। यदि किसी डिवाइस या कनेक्शन में समस्या आती है, तो संपूर्ण नेटवर्क बाधित हो सकता है।



4. मैश टोपोलॉजी (Mesh Topology):

इस प्रकार में हर डिवाइस अन्य सभी डिवाइसों से सीधे जुड़ा होता है। यह बहुत सुरक्षित और विश्वसनीय है, लेकिन इसे स्थापित करना महंगा और जटिल हो सकता है।



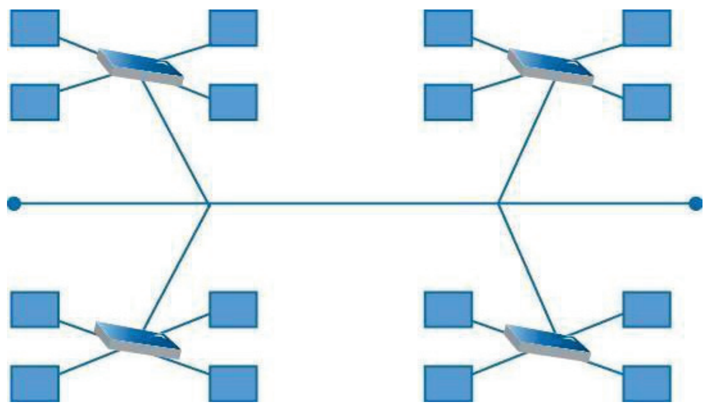
5. ट्री टोपोलॉजी (Tree Topology):

यह एक हाइब्रिड टोपोलॉजी है जिसमें एक मुख्य हब से कई उप-हब जुड़े होते हैं। यह संरचना स्टार और बस टोपोलॉजी का संयोजन होती है।

6. हाइब्रिड टोपोलॉजी (Hybrid Topology):

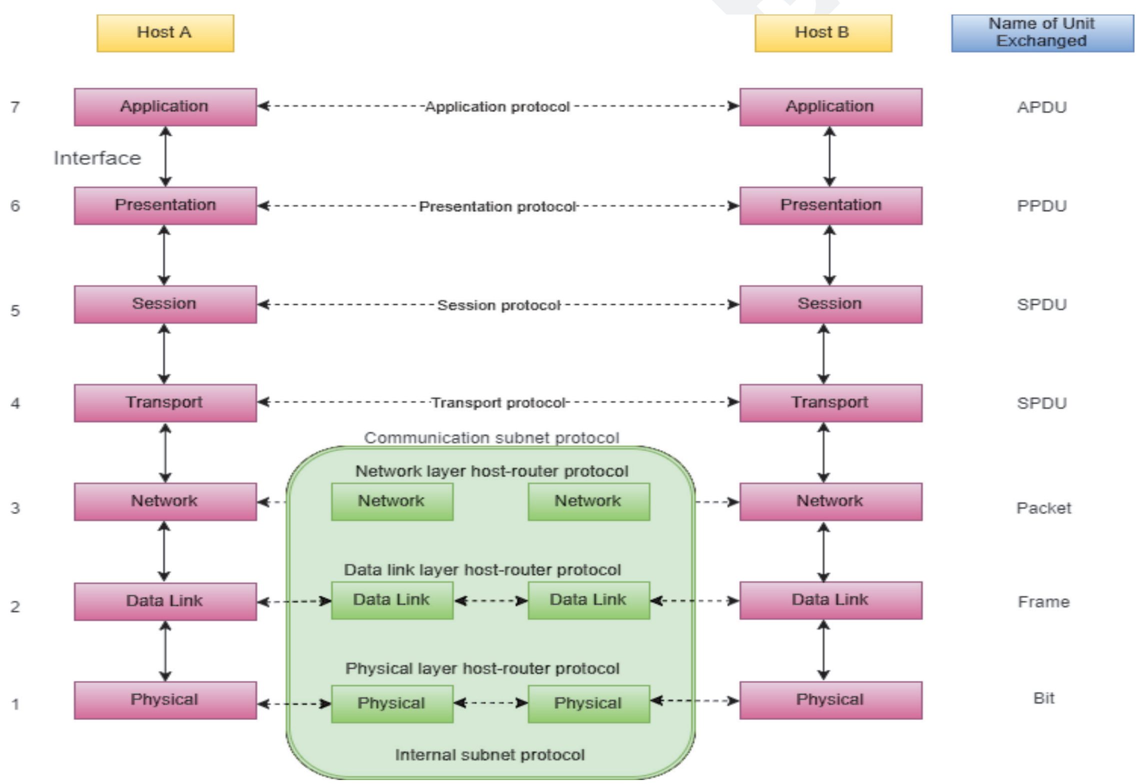
इसमें विभिन्न प्रकार की टोपोलॉजी का मिश्रण होता है। यह नेटवर्क की आवश्यकताओं के अनुसार विभिन्न टोपोलॉजी के फायदे को एक साथ लाती है।

SCERT DELHI



1.6 OSI Model

OSI मॉडल (Open Systems Interconnection Model) एक संदर्भ मॉडल है जो नेटवर्क संचार के विभिन्न स्तरों को परिभाषित करता है। इसे सात स्तरों में विभाजित किया गया है, जो डेटा ट्रांसफर के लिए आवश्यक प्रक्रियाओं को समझाने में मदद करते हैं। यहाँ OSI मॉडल के सात स्तरों का संक्षिप्त विवरण दिया गया है:



फिजिकल लेयर (Physical Layer):

यह स्तर हार्डवेयर और फिजिकल माध्यमों से संबंधित है, जैसे कि केबल, स्विच, और हब। इसका काम डेटा ट्रांसमिशन के लिए इलेक्ट्रिकल सिग्नल बनाना और भेजना है।

डाटा लिंक लेयर (Data Link Layer):

यह स्तर नेटवर्क में डेटा फ्रेम बनाने और डेटा की त्रुटियों को नियंत्रित करने का काम करता है। यह MAC एड्रेसिंग और फ्लो कंट्रोल से संबंधित होता है।

नेटवर्क लेयर (Network Layer):

यह स्तर डेटा पैकेट्स को रूट करने का काम करता है। यह IP एड्रेसिंग और नेटवर्क ट्रैफिक को मैनेज करता है।

ट्रांसपोर्ट लेयर (Transport Layer):

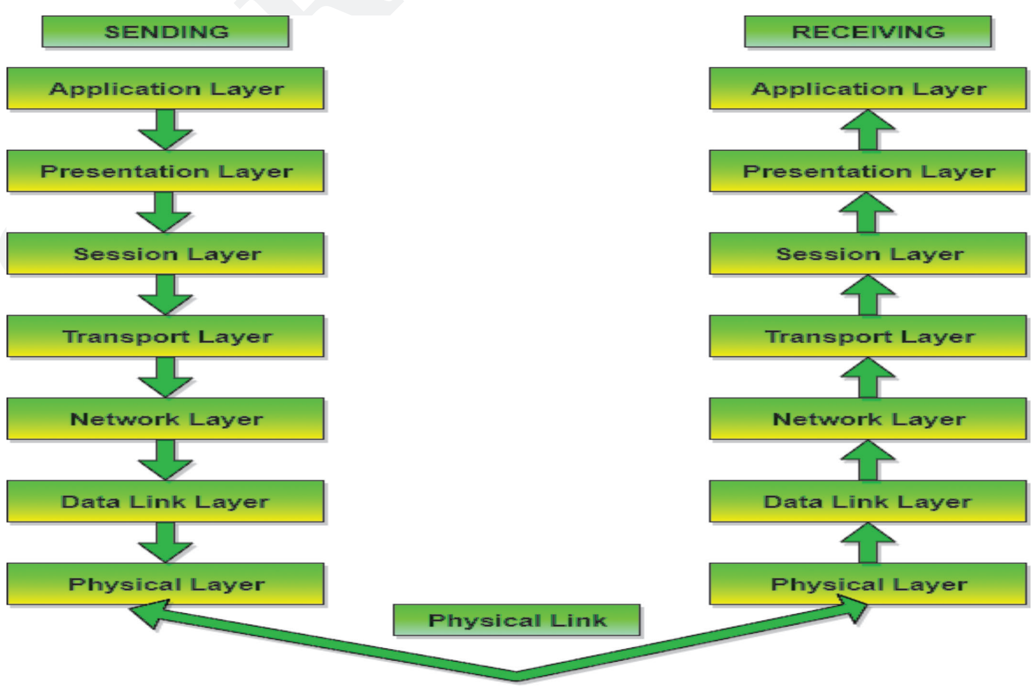
यह स्तर डेटा ट्रांसफर की विश्वसनीयता सुनिश्चित करता है। यह डेटा को छोटे हिस्सों (सेगमेंट) में बांटता है और रिसीवर तक सही तरीके से पहुंचाने की जिम्मेदारी लेता है। TCP और UDP इस स्तर पर काम करते हैं।

सेशन लेयर (Session Layer):

यह स्तर एप्लिकेशन के बीच संचार सत्रों का प्रबंधन करता है। यह कनेक्शन को स्थापित करता, बनाए रखता और समाप्त करता है।

प्रेजेंटेशन लेयर (Presentation Layer):

यह स्तर डेटा का स्वरूप निर्धारित करता है, जैसे कि एनकोडिंग, डिकोडिंग और डेटा की फॉर्मेटिंग। यह सुनिश्चित करता है कि डेटा को सही तरीके से प्रस्तुत किया जाए।



1.7 प्रोटोकॉल का सिद्धांत

नेटवर्किंग में प्रोटोकॉल एक नियमों और मानदंडों का सेट है जो निर्धारित करता है कि डेटा को नेटवर्क पर कैसे भेजा और प्राप्त किया जाएगा। प्रोटोकॉल डेटा के आदान-प्रदान की प्रक्रियाओं को परिभाषित करते हैं, जिससे संचार प्रभावी और कुशल होता है। प्रोटोकॉल के कुछ प्रमुख पहलू इस प्रकार हैं:

प्रोटोकॉल के प्रकार:

संचार प्रोटोकॉल: डिवाइस के बीच डेटा का आदान-प्रदान करने में मदद करते हैं (जैसे HTTP, FTP)।

ट्रांसपोर्ट प्रोटोकॉल: एंड-टू-एंड संचार का प्रबंधन करते हैं और डेटा की डिलीवरी सुनिश्चित करते हैं (जैसे TCP, UDP)।

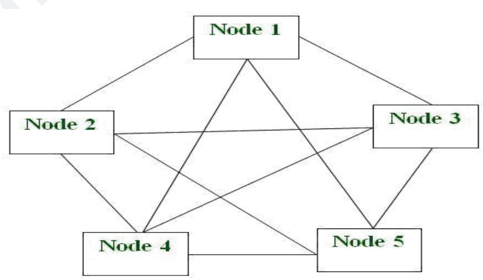
नेटवर्क प्रोटोकॉल: डेटा पैकेट्स की रूटिंग और एड्रेसिंग संभालते हैं (जैसे IP)।

ऐप्लिकेशन प्रोटोकॉल: ऐप्लिकेशन लेयर पर सेवाएँ प्रदान करते हैं (जैसे SMTP ईमेल के लिए)।

1.8 नेटवर्क तकनीकें

1. पीयर-टू-पीयर नेटवर्क: (Peer-to-Peer Network):

पीयर-टू-पीयर (P2P) नेटवर्क एक प्रकार का नेटवर्क आर्किटेक्चर है जहां सभी उपकरण (जिन्हें नोड्स या पीयर्स कहा जाता है) समान रूप से काम करते हैं और डेटा साझा करते हैं। इसमें कोई केंद्रीय सर्वर नहीं होता, और सभी नोड्स स्वतंत्र रूप से एक-दूसरे से संवाद कर सकते हैं।



P2P Architecture

2. क्लाइंट और सर्वर नेटवर्क

क्लाइंट और सर्वर नेटवर्क एक ऐसा नेटवर्क आर्किटेक्चर है जिसमें दो प्रमुख घटक होते हैं: क्लाइंट और सर्वर। इस मॉडल में सर्वर केंद्रित होता है और क्लाइंट इसके संसाधनों और सेवाओं का उपयोग करते हैं। आइए इसे विस्तार से समझते हैं:

विशेषताएँ:

1. क्लाइंट:

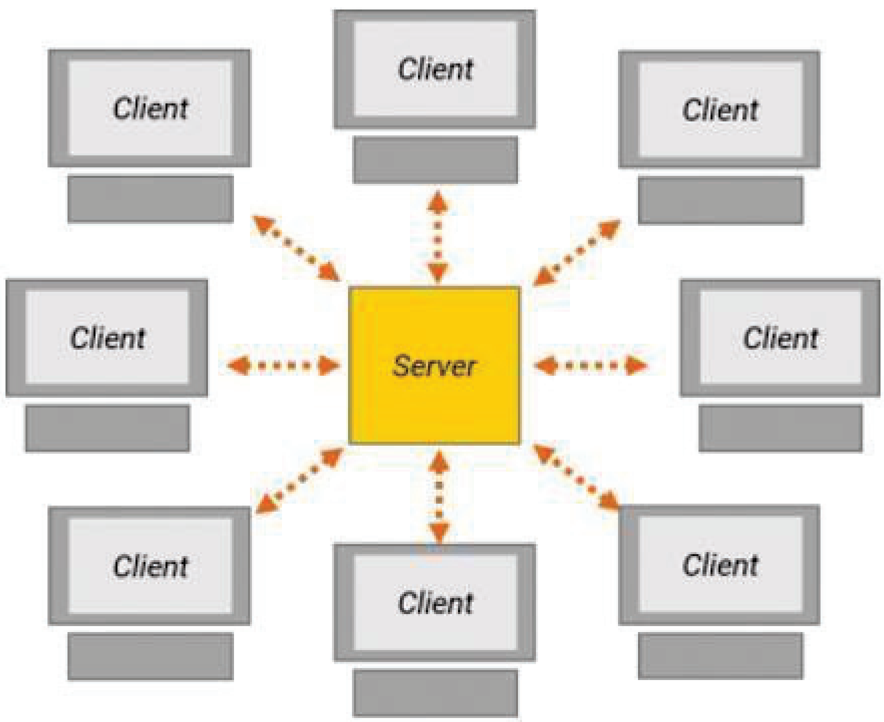
क्लाइंट वे उपकरण होते हैं (जैसे कंप्यूटर, स्मार्टफोन) जो सर्वर से सेवाएँ या संसाधन मांगते हैं।

क्लाइंट नेटवर्क पर सर्वर से जानकारी प्राप्त करने के लिए अनुरोध भेजते हैं।

2. सर्वर:

सर्वर एक उच्च शक्ति वाला कंप्यूटर या मशीन होती है जो डेटा, सेवाएँ, और संसाधन प्रदान करती है।

सर्वर क्लाइंट के अनुरोधों को संभालता है और आवश्यक डेटा या सेवाएँ लौटाता है।



1.9 डेटा ट्रांसमिशन

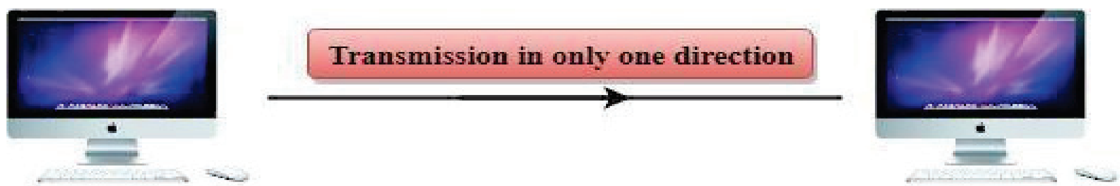
डेटा ट्रांसमिशन से तात्पर्य है कि डेटा को एक स्थान से दूसरे स्थान पर भेजने की प्रक्रिया। यह कंप्यूटर नेटवर्किंग और संचार का एक महत्वपूर्ण पहलू है। डेटा ट्रांसमिशन विभिन्न माध्यमों के माध्यम से हो सकता है, जैसे वायर्ड (तारयुक्त) और वायरलेस (ताररहित)।

डेटा ट्रांसमिशन मोड को तीन श्रेणियों में विभाजित किया जाता है:

1. सिंप्लेक्स मोड (Simplex Mode):

परिभाषा: इस मोड में डेटा केवल एक दिशा में भेजा जाता है। एक डिवाइस डेटा भेजता है और दूसरा केवल उसे प्राप्त करता है।

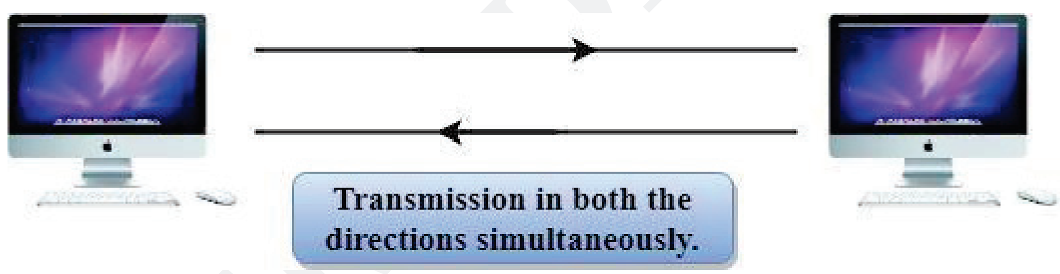
उदाहरण - जैसे टेलीविजन प्रसारण, जहाँ टीवी सेट केवल डेटा प्राप्त करता है और प्रसारक केवल डेटा भेजता है।



2. डुप्लेक्स मोड (Duplex Mode):

परिभाषा: इस मोड में डेटा दोनों दिशाओं में एक साथ भेजा जा सकता है। इसे पूर्ण द्विदिश संचार कहा जाता है।

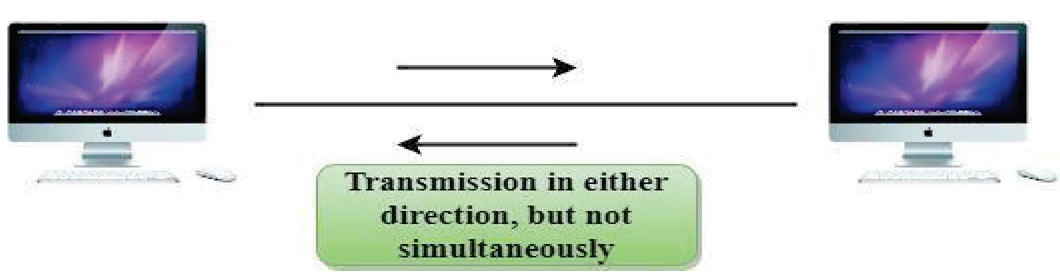
उदाहरण - जैसे टेलीफोन कॉल, जहाँ दोनों पक्ष एक साथ बोल और सुन सकते हैं।



3. हाफ डुप्लेक्स मोड (Half Duplex Mode):

परिभाषा: इस मोड में डेटा दोनों दिशाओं में भेजा जा सकता है, लेकिन एक समय में केवल एक दिशा में। यानी, एक डिवाइस या तो भेज सकता है या प्राप्त कर सकता है, लेकिन दोनों नहीं।

उदाहरण - जैसे वॉकी-टॉकी, जहाँ एक व्यक्ति बोलता है और दूसरा सुनता है, लेकिन दोनों एक साथ नहीं बोल सकते।



अपनी प्रगति जाँचे

अ. बहुविकल्पीय प्रश्न

1. किस परत का मुख्य कार्य डेटा पैकेट्स को भेजना और प्राप्त करना है?

A) एप्लिकेशन लेयर B) ट्रांसपोर्ट लेयर
C) नेटवर्क लेयर D) फिजिकल लेयर

2. किस OSI परत में डेटा को एन्क्रिप्ट किया जाता है?

A) एप्लिकेशन लेयर B) प्रेज़ेंटेशन लेयर
C) सेशन लेयर D) नेटवर्क लेयर

3. नीचे दिए गए में से कौन-सी परत एक टर्मिनल और एक एप्लिकेशन के बीच संचार को नियंत्रित करती है?

A) फिजिकल लेयर B) सेशन लेयर
C) डेटा लिंक लेयर D) ट्रांसपोर्ट लेयर

4. नीचे दिए गए में से कौन-सी टोपोलॉजी सभी उपकरणों को एक ही केबल में जोड़ती है?

A) स्टार टोपोलॉजी B) रिंग टोपोलॉजी
C) बस टोपोलॉजी D) मैष टोपोलॉजी

5. स्टार टोपोलॉजी में डेटा किसके माध्यम से भेजा जाता है?

A) सभी उपकरणों के बीच सीधे B) केंद्रीय स्विच या हब के माध्यम से
C) एक सर्कल में D) एक एकल केबल में

6. किस उपकरण का उपयोग विभिन्न नेटवर्क के बीच डेटा पैकेट्स को रूट करने के लिए किया जाता है?

A) स्विच B) राउटर
C) हब D) मोडेम

7. किस नेटवर्क उपकरण का मुख्य कार्य एक ही नेटवर्क पर डेटा को विभिन्न डिवाइसों में वितरित करना है?

SCERT DELHI

A) राउटर B) स्विच

C) हब D) फायरवॉल

8. किस प्रोटोकॉल का उपयोग ईमेल भेजने के लिए किया जाता है?

A) FTP B) SMTP

C) SNMP D) ICMP

9. किस प्रकार का नेटवर्क छोटे क्षेत्र में, जैसे कि घर या ऑफिस में, उपकरणों को जोड़ने के लिए प्रयोग किया जाता है?

A) WAN B) LAN

C) MAN D) PAN

10. किस प्रकार की नेटवर्किंग तकनीक में डेटा को छोटे पैकेट में विभाजित किया जाता है?

A) सर्किट-स्विचिंग B) पैकेट-स्विचिंग

C) टेम्परी-स्विचिंग D) थ्रेड-स्विचिंग

ब. लघु उत्तरीय प्रश्न

1. OSI मॉडल में कुल कितनी परतें होती हैं?
2. कौन-सी परत डेटा को एन्क्रिप्ट करती है?
3. नेटवर्क लेयर का मुख्य कार्य क्या है?
4. कौन-सी परत एप्लिकेशन को नेटवर्क से जोड़ती है?
5. राउटर का मुख्य कार्य क्या है?
6. स्विच और हब में क्या अंतर
7. फायरवॉल का कार्य क्या होता है?
8. मोडेम का उपयोग किस लिए किया जाता है?
9. एक्सेस प्वाइंट क्या करता है?
10. स्टार टोपोलॉजी का मुख्य लाभ क्या है?

SCERT DELHI

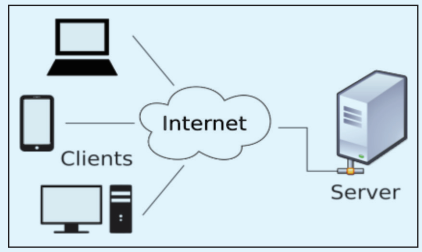
विंडोज सर्वर की स्थापना और कॉन्फ़िगरेशन

अध्याय 2

परिचय

Windows Server (विंडोज सर्वर):

Windows Server माइक्रोसॉफ्ट का एक सर्वर ऑपरेटिंग सिस्टम है, जो नेटवर्क मैनेजमेंट, डेटा स्टोरेज और एप्लिकेशन होस्टिंग के लिए उपयोग किया जाता है। इसका उपयोग बड़े नेटवर्क, डेटा सेंटर और क्लाउड इंफ्रास्ट्रक्चर में होता है।



Regular Windows और Windows Server में अंतर:

1. **उद्देश्य (Purpose):**

   Regular Windows: व्यक्तिगत उपयोग के लिए (जैसे, लैपटॉप/डेस्कटॉप)।

   Windows Server: सर्वर और नेटवर्क प्रबंधन के लिए।

2. **यूजर इंटरफेस (User Interface):**

   Regular Windows: उपयोगकर्ता-अनुकूल, मल्टीमीडिया सुविधाओं के साथ।

   Windows Server: सरल इंटरफेस, एडमिन टास्क के लिए।

3. **यूजर सीमा (User Limits):**

   Regular Windows: 1-2 यूजर्स के लिए।

   Windows Server: कई यूजर्स, नेटवर्क पर कई डिवाइस कनेक्शन।

4. **हार्डवेयर सपोर्ट (Hardware Support):**

   Regular Windows: मध्यम स्तर का हार्डवेयर सपोर्ट।

   Windows Server: हाई-एंड हार्डवेयर सपोर्ट (अधिक RAM, CPU)।

5. नेटवर्क प्रबंधन (Network Management):

Regular Windows: बेसिक नेटवर्किंग।

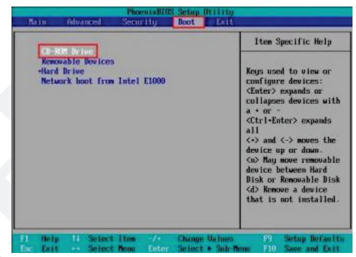
Windows Server: Active Directory, DNS, DHCP जैसी सेवाओं के साथ एडवांस नेटवर्किंग।

Windows Server 2012 की इंस्टॉलेशन का स्टेप-बाय-स्टेप प्रोसेस

1. Boot Setup:

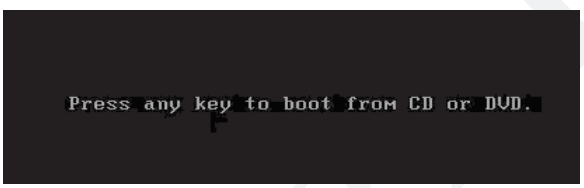
DvD या USB ड्राइव को कंप्यूटर में इंसर्ट करें।

सिस्टम को रीस्टार्ट करें और BIOS/UEFI में जाकर बूट डिवाइस को सेट करें (USB या DvD)।



2. Install Setup:

बूट होने पर "Press any key to boot from CD or DvD" संदेश दिखाई देगा, कोई भी बटन दबाएँ।



3. Language & Preferences:

Language, Time, और Keyboard Layout चुनें, फिर Next पर क्लिक करें।

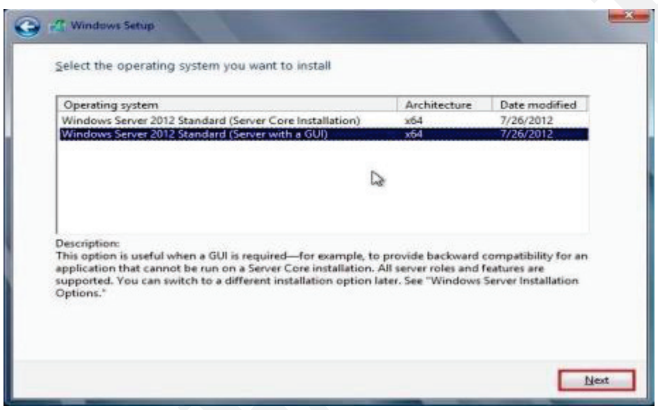
4. Install Now:

"Install Now" पर क्लिक करें।

5. Select Windows version:

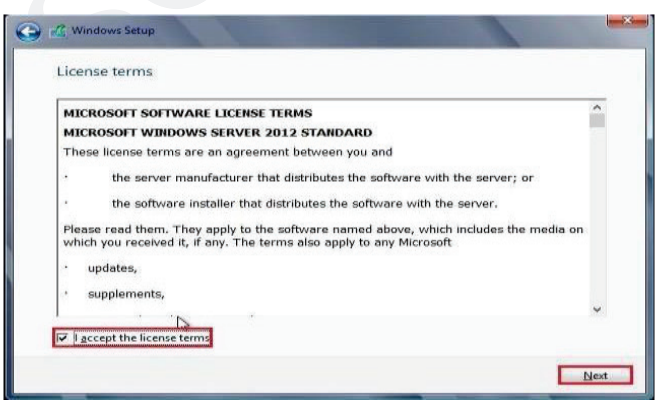
Windows Server 2012 के संस्करण (Standard, Datacenter आदि) को चुनें।

Next पर क्लिक करें।



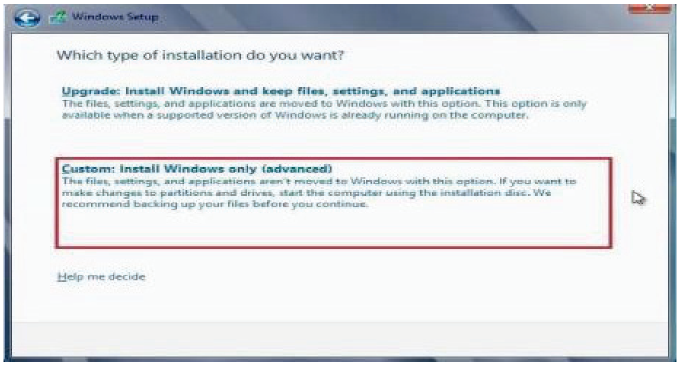
6. License Terms:

लाइसेंस एग्रीमेंट को स्वीकार करें और Next पर क्लिक करें।



7. Installation Type:

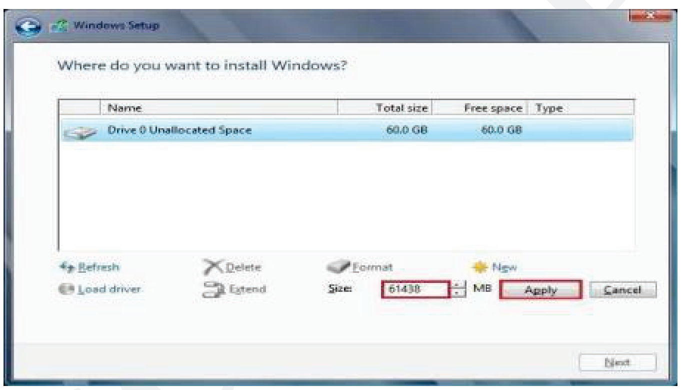
यदि क्लीन इंस्टॉलेशन कर रहे हैं, तो Custom: Install Windows only (Advanced) चुनें।



8. Partition Setup:

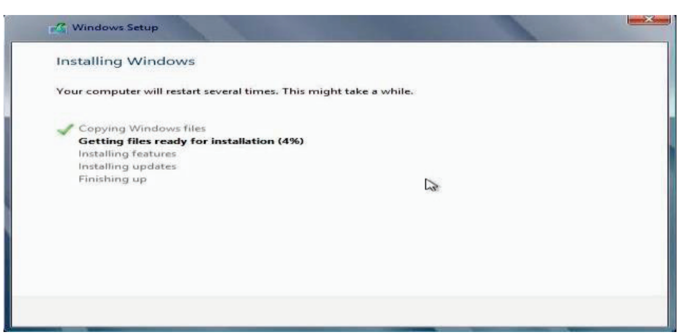
इंस्टॉलेशन के लिए हार्ड ड्राइव या पार्टिशन को चुनें। अगर जरूरत हो, तो नया पार्टिशन बना सकते हैं।

Next पर क्लिक करें।



9. Installation Process:

Windows Server की फाइलें और कॉपी इंस्टॉल होंगी। यह प्रक्रिया कुछ मिनटों तक चलेगी।

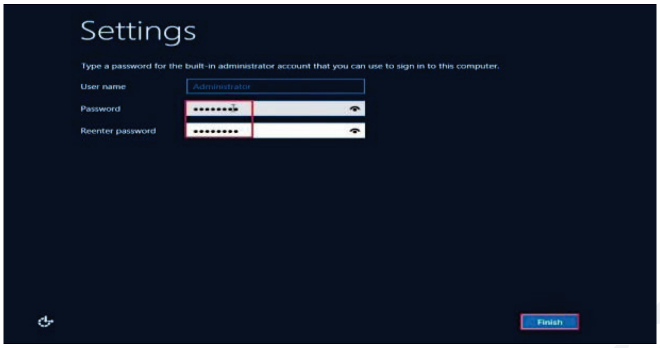


10. Restart:

इंस्टॉलेशन कंप्लीट होने पर सिस्टम अपने आप रीस्टार्ट होगा।

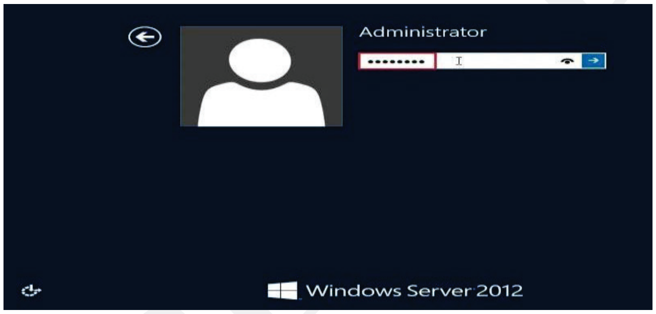
11. Configure Settings:

सिस्टम के रीस्टार्ट होने के बाद, आपको Administrator Password सेट करने का विकल्प मिलेगा। पासवर्ड दर्ज करें।



12. Login:

पासवर्ड सेट करने के बाद, Ctrl+Alt+Delete दबाएँ और लॉग इन करें।



Windows Server पर पोस्ट-इंस्टॉलेशन कार्य:

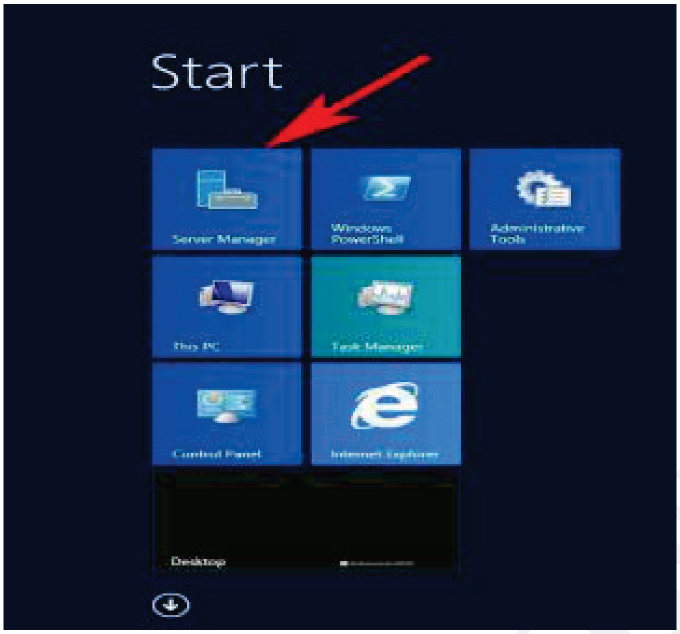
1. सर्वर का नाम बदलना (Change Server Name)

Server Manager खोलें।

Local Server पर जाएं।

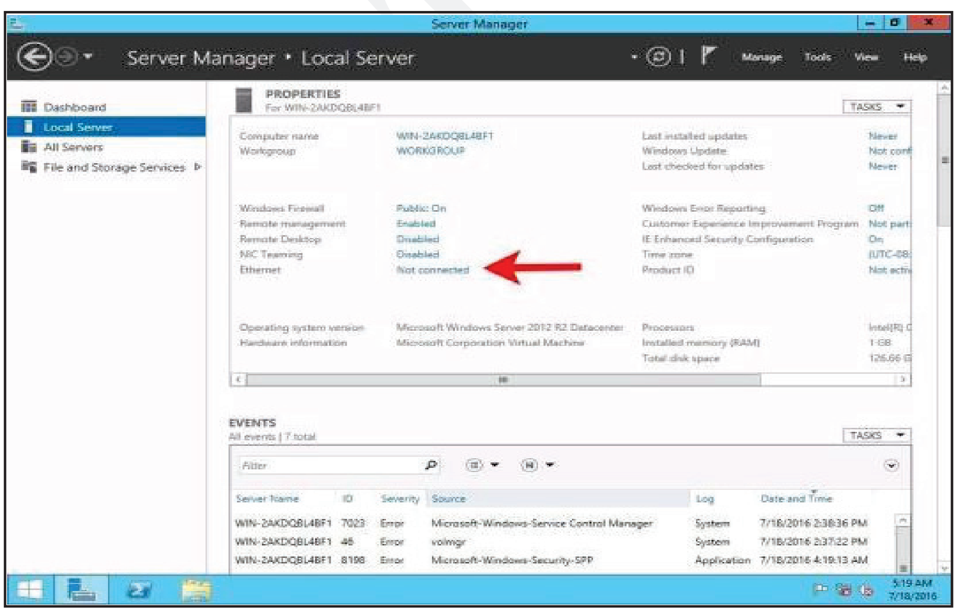
Computer Name विकल्प पर क्लिक करके नया नाम सेट करें।

सिस्टम को रिबूट करें।

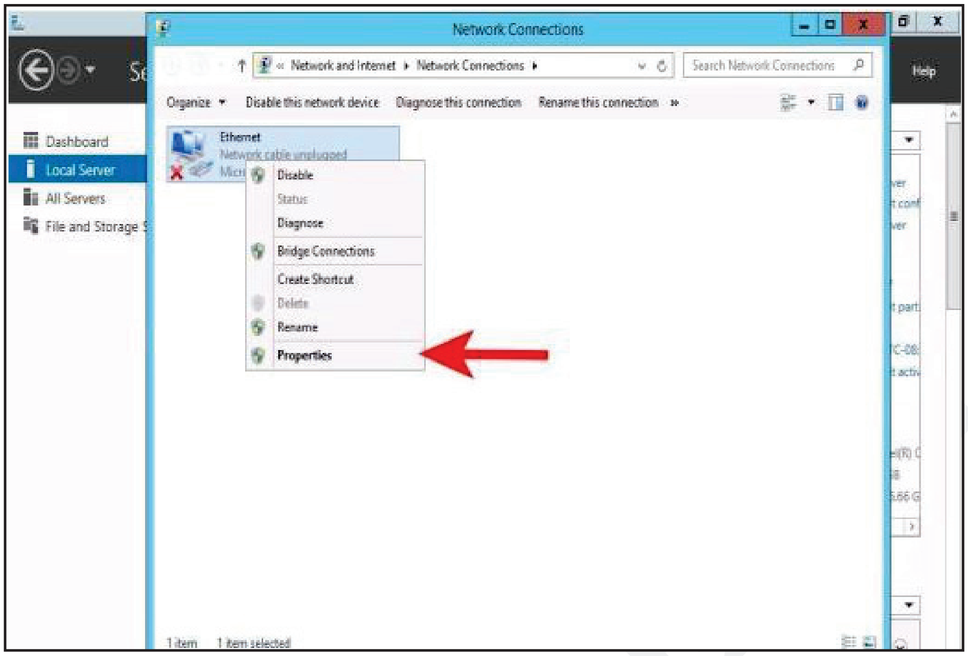


2. IP एड्रेस सेट करना (Set Static IP Address)

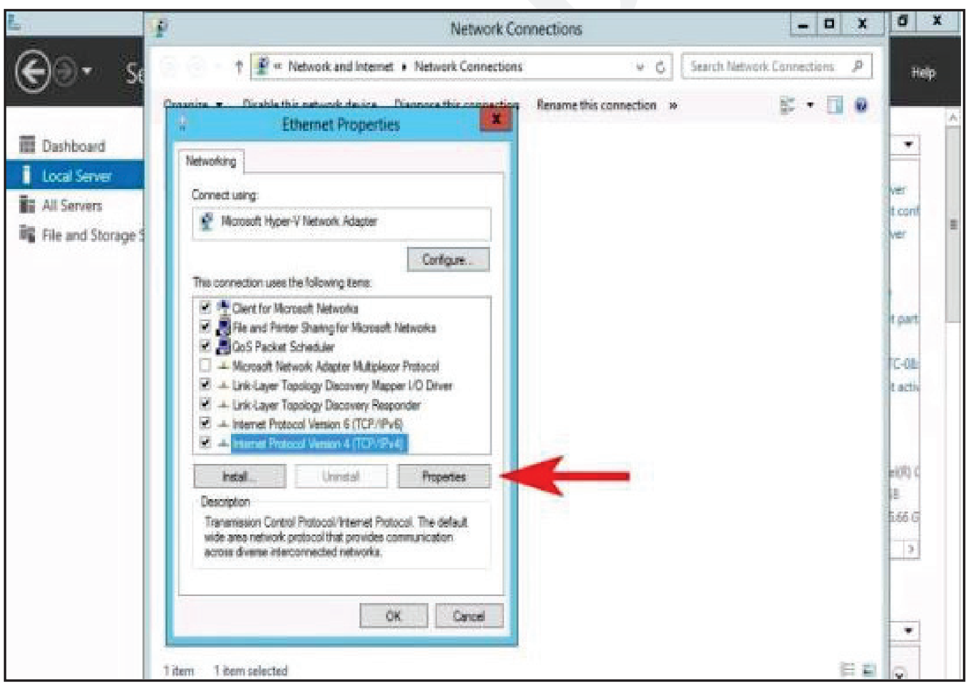
Control Panel Network and Sharing Center Change Adapter Settings।

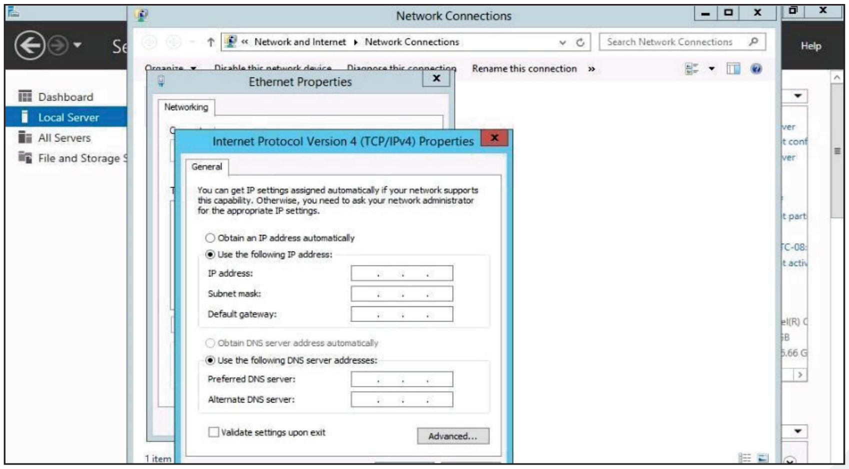


Ethernet पर राइट-क्लिक करें और Properties चुनें।



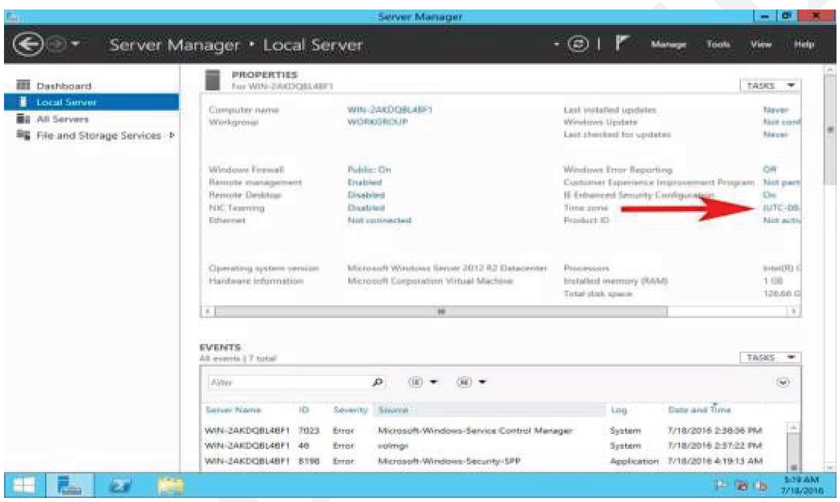
IPv4 विकल्प में जाकर मैन्युअली IP एड्रेस डालें।



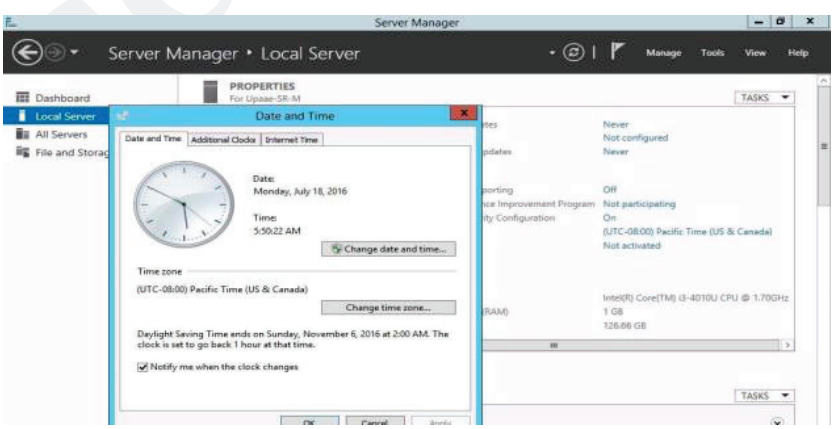


3. टाइम ज़ोन सेट करना (Set Time Zone)

Control Panel Date and Time।



Time Zone सेट करें और सही टाइम ज़ोन चुनें।



4. Windows Updates इंस्टॉल करना

Settings Update & Security Check for Updates

सभी आवश्यक अपडेट इंस्टॉल करें

5. रोल्स और फीचर्स जोड़ना (Add Roles and Features)

Server Manager Add Roles and Features

ज़रूरी रोल्स और फीचर्स चुनें और इंस्टॉल करें

6. फायरवॉल सेटिंग्स कॉन्फ़िगर करना (Configure Firewall)

Windows Defender Firewall Advanced Settings

इनकमिंग और आउटगोइंग ट्रैफिक के लिए नियम सेट करें

7. रिमोट डेस्कटॉप सक्षम करना (Enable Remote Desktop)

Server Manager Local Server Remote Desktop विकल्प को Enabled करें

Windows Server 2012 को प्रबंधित करना

2.1 Windows Server 2012 प्रबंधन का अवलोकन

Windows Server 2012 एक शक्तिशाली ऑपरेटिंग सिस्टम है जिसे नेटवर्क, एप्लिकेशन और इंफ्रास्ट्रक्चर के प्रबंधन के लिए डिज़ाइन किया गया है। यह कई नई सुविधाएँ और सुधार प्रदान करता है जो सर्वर और वर्चुअल वातावरण के प्रबंधन को आसान और अधिक कुशल बनाते हैं।

2.2 Windows PowerShell का परिचय

Windows PowerShell एक कमांड-लाइन शेल और स्क्रिप्टिंग भाषा है जिसे सिस्टम प्रशासन और ऑटोमेशन कार्यों को आसान और तेज़ बनाने के लिए विकसित किया गया है। इसे विशेष रूप से Microsoft द्वारा Windows सिस्टम के प्रबंधन के लिए डिज़ाइन किया गया है।

SCERT DELHI

2.2.1 कमांड-लाइन शेल (Command-line shell)

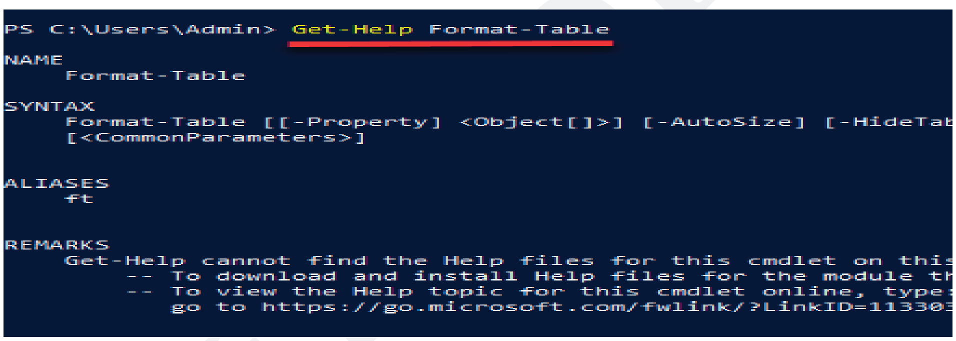
कमांड-लाइन शेल एक इंटरफेस है जो यूज़र्स को टेक्स्ट के रूप में कमांड टाइप करके ऑपरेटिंग सिस्टम से बातचीत करने की सुविधा देता है। ग्राफिकल यूज़र इंटरफेस (GUI) के विपरीत, इसमें सभी निर्देश सीधे कमांड के रूप में इनपुट किए जाते हैं।

2.2.2 स्क्रिप्टिंग भाषा (Scripting Language)

स्क्रिप्टिंग भाषा एक प्रोग्रामिंग भाषा होती है जिसका उपयोग स्वचालित (automate) कार्यों को करने के लिए किया जाता है। ये भाषाएँ प्रोग्राम को सीधे चलाने के लिए डिज़ाइन की गई होती हैं, बिना किसी कंपाइलिंग (compilation) के।

इंटरप्रेटेड: स्क्रिप्टिंग भाषाएँ सीधे रनटाइम पर इंटरप्रेटर द्वारा निष्पादित की जाती हैं, यानी इन्हें पहले से कंपाइल करने की आवश्यकता नहीं होती।

ऑटोमेशन: इनका उपयोग दोहराए जाने वाले कार्यों को स्वचालित करने के लिए किया जाता है, जैसे सर्वर प्रशासन, वेब पेज की स्क्रिप्टिंग, डेटा प्रोसेसिंग आदि।



```
PS C:\Users\Admin> Get-Help Format-Table

NAME
    Format-Table

SYNTAX
    Format-Table [[-Property] <Object[]>] [-AutoSize] [-HideTab
    [<CommonParameters>]

ALIASES
    ft

REMARKS
    Get-Help cannot find the Help files for this cmdlet on this
        -- To download and install Help files for the module th
        -- To view the Help topic for this cmdlet online, type:
           go to https://go.microsoft.com/fwlink/?LinkID=11330
```

2.2.3 ऑटोमेशन प्लेटफ़ॉर्म (Automation platform)

PowerShell की विस्तारशील प्रकृति (extensible nature) ने एक ऐसा इकोसिस्टम तैयार किया है जिसमें PowerShell मॉड्यूल्स का उपयोग करके लगभग किसी भी तकनीक को तैनात (deploy) और प्रबंधित (manage) किया जा सकता है जिसके साथ आप काम करते हैं।

* Microsoft (माइक्रोसॉफ्ट)
* Azure
* Windows
* Exchange

* SQL
* Third-party (तृतीय पक्ष)
* AWS
* vMWare
* Google Cloud

कॉन्फ़िगरेशन प्रबंधन (Configuration management)

PowerShell Desired State Configuration (DSC) PowerShell में एक प्रबंधन ढांचा है जो आपको अपने एंटरप्राइज इंफ्रास्ट्रक्चर का प्रबंधन कोड के रूप में कॉन्फ़िगरेशन के साथ करने की सुविधा देता है। DSC के साथ, आपः

घोषणात्मक कॉन्फ़िगरेशन और कस्टम स्क्रिप्ट बनाएं ताकि पुनरावृत्त तैनाती (repeatable deployments) की जा सके।

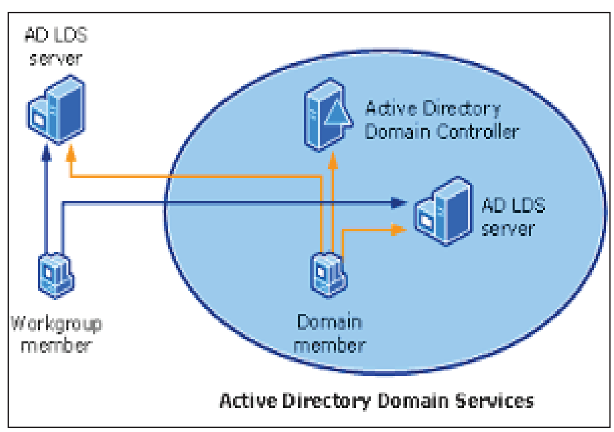
कॉन्फ़िगरेशन सेटिंग्स को लागू करें और कॉन्फ़िगरेशन ड्रिफ्ट की रिपोर्ट करें।

कॉन्फ़िगरेशन को पुश या पुल मॉडल का उपयोग करके तैनात करें।

3. Active Directory Domain Services को इंस्टॉल और कॉन्फ़िगर करें

3.1 Active Directory Domain Services का अवलोकनः

Active Directory Domain Services (AD DS) एक Microsoft तकनीक है जो नेटवर्क में यूज़र्स, कंप्यूटर, और अन्य संसाधनों का प्रबंधन और नियंत्रण करती है। यह एक केंद्रीय डेटाबेस प्रदान करती है जिसमें सभी नेटवर्क तत्वों की जानकारी होती है।



मुख्य विशेषताएँः

1. केंद्रित प्रबंधनः

AD DS एक केंद्रीय स्थान पर सभी यूज़र्स, ग्रुप्स, कंप्यूटर और अन्य नेटवर्क संसाधनों की जानकारी संग्रहित करता है, जिससे उन्हें प्रबंधित करना आसान होता है।

SCERT DELHI

2. उपयोगकर्ता प्रमाणीकरण:

AD DS यूज़र्स को नेटवर्क में लॉग इन करने और संसाधनों तक पहुंच प्राप्त करने के लिए प्रमाणीकरण करता है, जिससे सुरक्षा सुनिश्चित होती है।

3. संगठनात्मक संरचना:

यह OU (Organizational Units) और डोमेन का उपयोग करके नेटवर्क संसाधनों को एक सुव्यवस्थित तरीके से व्यवस्थित करता है, जिससे पॉलिसी प्रबंधन सरल होता है।

4. ग्रुप पॉलिसी प्रबंधन:

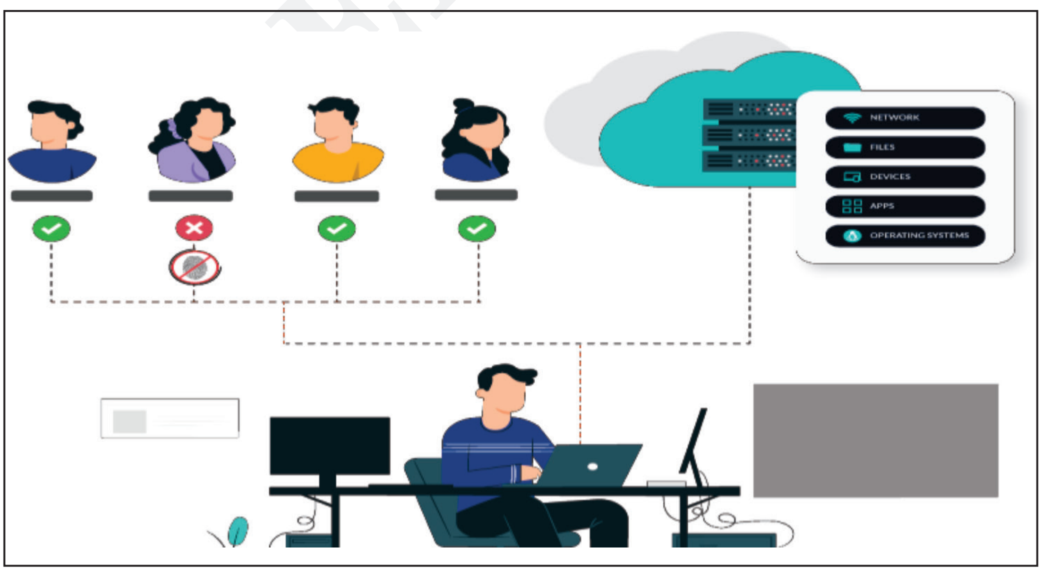
AD DS के माध्यम से, व्यवस्थापक ग्रुप पॉलिसीज़ सेट कर सकते हैं, जो यूज़र्स और कंप्यूटर पर सुरक्षा और कॉन्फ़िगरेशन सेटिंग्स को लागू करती हैं।

5. स्केलेबिलिटी:

यह बड़े नेटवर्क को संभालने में सक्षम है, जिससे संगठनों की बढ़ती आवश्यकताओं के अनुसार इसे बढ़ाया जा सकता है।

3.2 डोमेन कंट्रोलर्स (Domain Controllers) का अवलोकन

डोमेन कंट्रोलर (Domain Controller) एक सर्वर है जो Active Directory Domain Services (AD DS) को चलाता है और नेटवर्क में यूज़र्स और कंप्यूटर के प्रमाणीकरण (authentication) और अधिकृत (authorization) का कार्य करता है। यह नेटवर्क के भीतर सभी सुरक्षा नीतियों और सेटिंग्स को लागू करने में महत्वपूर्ण भूमिका निभाता है।



मुख्य विशेषताएँ:

1. **प्रमाणीकरण:**

   डोमेन कंट्रोलर यूज़र्स और कंप्यूटर की पहचान को सत्यापित करता है, जिससे उन्हें नेटवर्क संसाधनों तक सुरक्षित पहुँच मिलती है।

2. **डेटाबेस प्रबंधन:**

   यह Active Directory में संग्रहीत जानकारी को प्रबंधित करता है, जिसमें यूज़र अकाउंट्स, ग्रुप्स, और अन्य नेटवर्क संसाधनों का डेटा शामिल होता है।

3. **मल्टीपल डोमेन कंट्रोलर्स:**

   एक संगठन में कई डोमेन कंट्रोलर्स हो सकते हैं, जो लोड बैलेंसिंग और फॉल्ट टॉलरेंस प्रदान करते हैं, ताकि यदि एक कंट्रोलर फेल हो जाए, तो अन्य उसे संभाल सके।

4. **ग्रुप पॉलिसी:**

   डोमेन कंट्रोलर ग्रुप पॉलिसी ऑब्जेक्ट्स (GPOs) को लागू करता है, जो यूज़र्स और कंप्यूटरों पर सुरक्षा सेटिंग्स और कॉन्फ़िगरेशन को नियंत्रित करती है।

5. **रेप्लिकेशन:**

   डोमेन कंट्रोलर्स के बीच डेटा रेप्लिकेशन सुनिश्चित करता है, ताकि सभी कंट्रोलर्स पर अद्यतन जानकारी समान हो।

3.3 डोमेन कंट्रोलर इंस्टॉल करना

डोमेन कंट्रोलर (Domain Controller) को इंस्टॉल करने के लिए निम्नलिखित चरणों का पालन करें:

इंस्टॉलेशन प्रक्रिया:

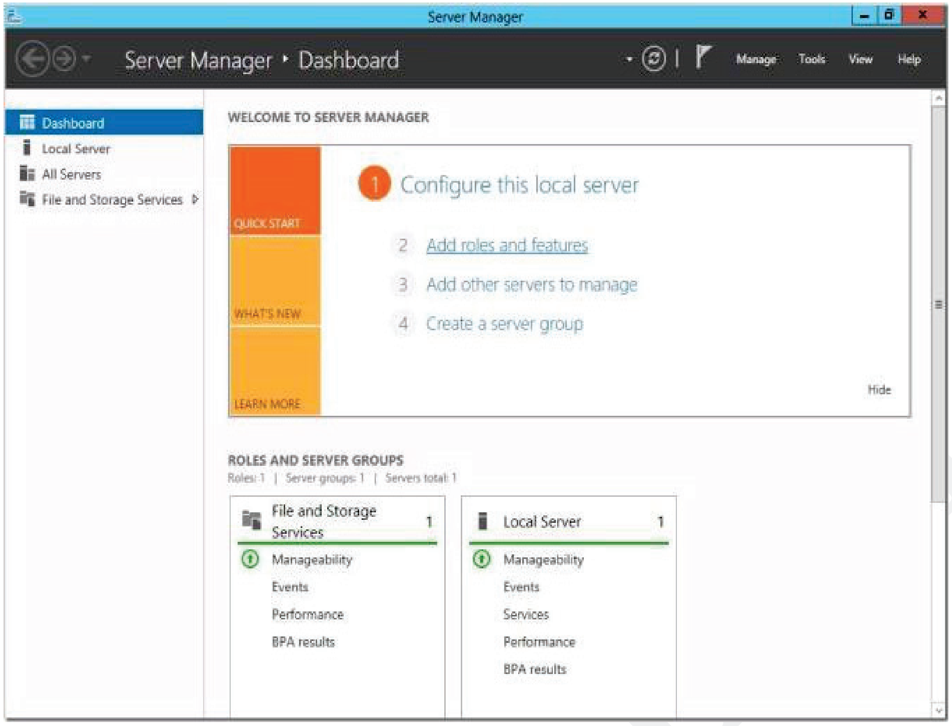
1. **Server Manager खोलें:**

   Windows Server में Server Manager को ओपन करें।

2. **Add Roles and Features:**

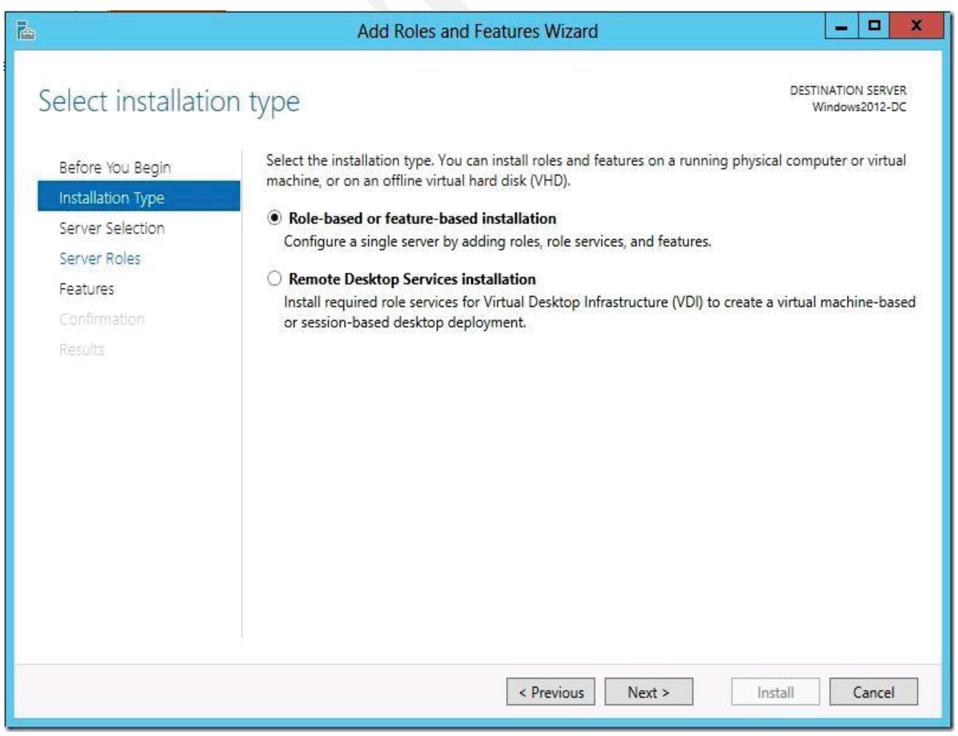
   'Manage' पर क्लिक करें और 'Add Roles and Features' का चयन करें।

SCERT DELHI



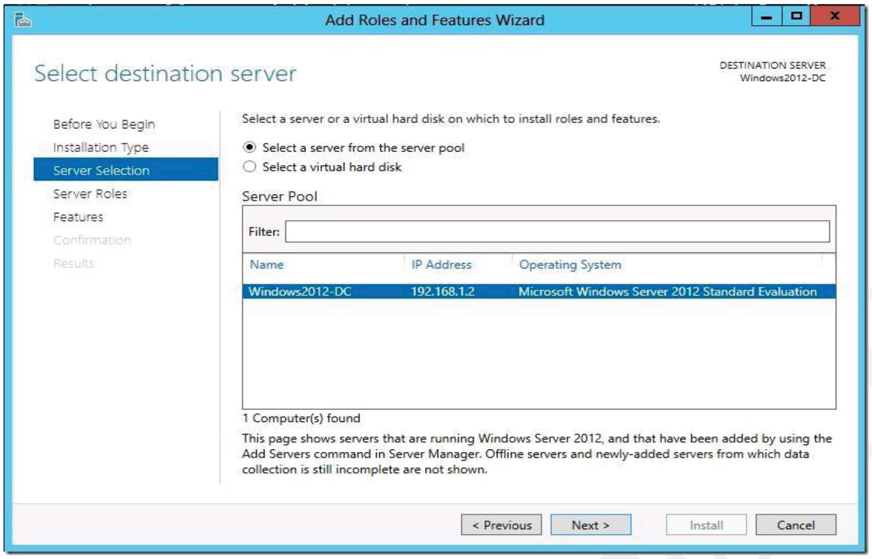
3. Role-Based Installation:

'Role-based or feature-based installation' का चयन करें और Next पर क्लिक करें।



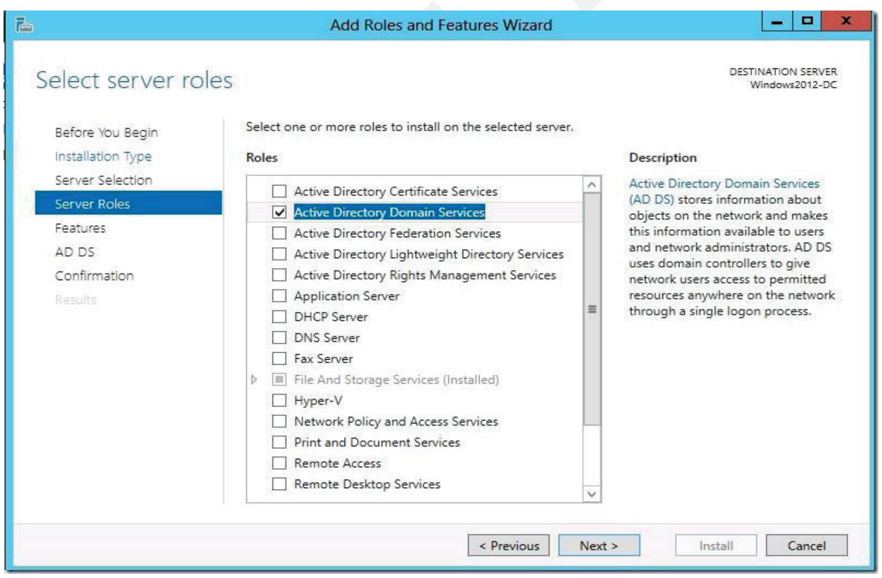
4. सर्वर का चयन करें:

उस सर्वर का चयन करें जिस पर आप डोमेन कंट्रोलर इंस्टॉल करना चाहते हैं।



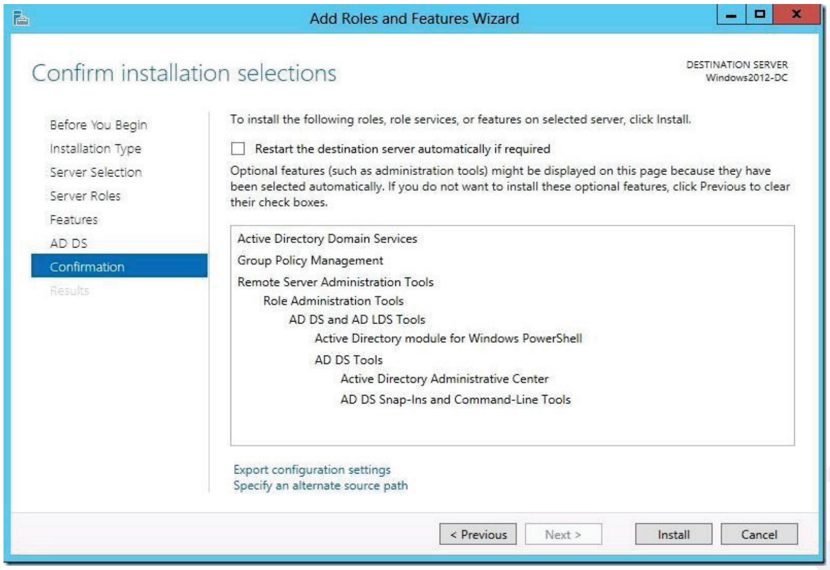
5. Active Directory Domain Services का चयन करें:

'Active Directory Domain Services' रोल को चुनें और Next पर क्लिक करें।



6. इंस्टॉलेशन को पूरा करें:

आवश्यक फीचर्स का चयन करें और इंस्टॉलेशन को पूरा करें। इंस्टॉलेशन के बाद, आपको AD DS को कॉन्फ़िगर करने के लिए एक सूचना मिलेगी।



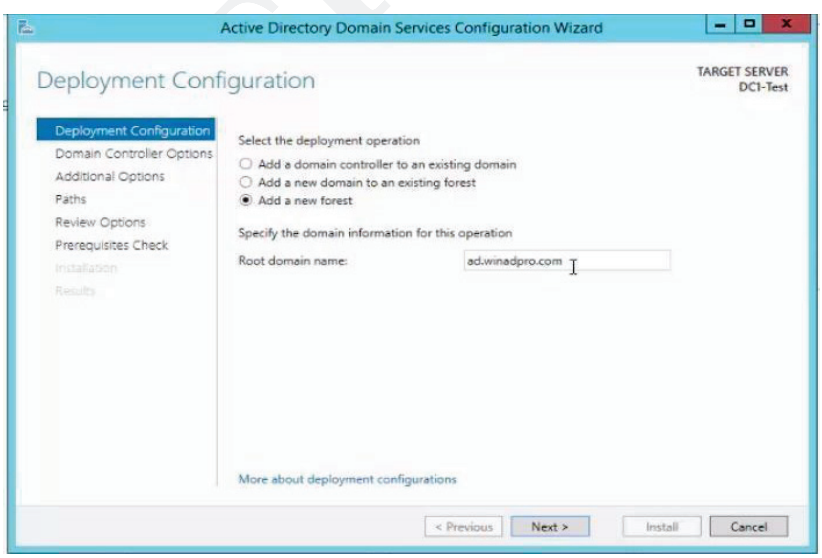
कॉन्फ़िगरेशन प्रक्रिया:

1. **Promote this server to a domain controller:**

   इंस्टॉलेशन के बाद, Server Manager में एक नोटिफिकेशन आएगा। 'Promote this server to a domain controller' पर क्लिक करें।

2. **Domain Configuration:**

   नया डोमेन बनाने के लिए 'Add a new forest' का चयन करें और डोमेन का नाम दें (उदाहरण - example.com)।

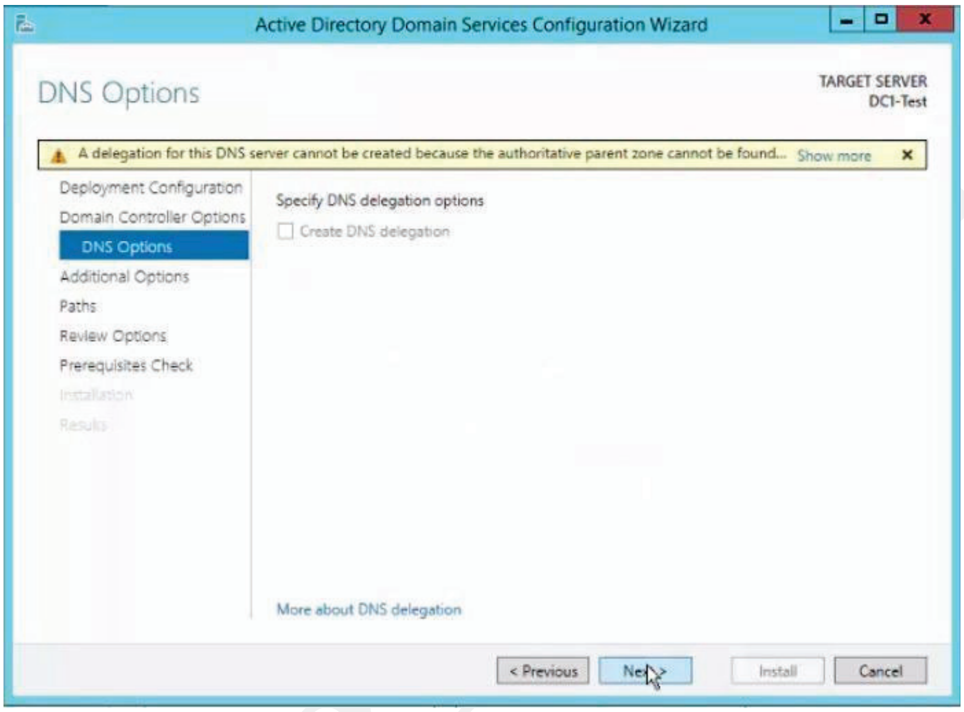


3. Domain Controller Options:

डोमेन कंट्रोलर के लिए आवश्यक विकल्प चुनें, जैसे कि DSRM पासवर्ड सेट करें।

4. DNS Configuration:

DNS सर्वर की सेटिंग्स कॉन्फ़िगर करें यदि आवश्यक हो।

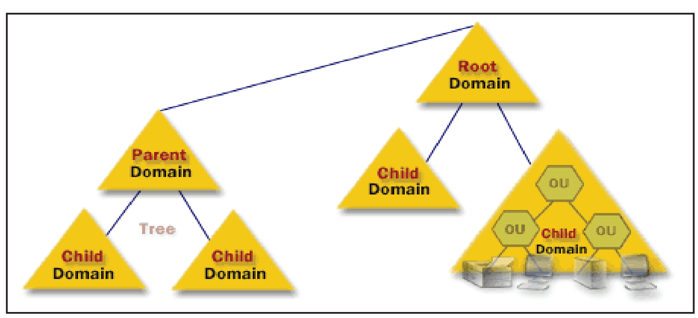


5. Review और Install:

सभी सेटिंग्स की समीक्षा करें और 'Install' पर क्लिक करें। सर्वर पुनरारंभ होगा।

3.4 Active Directory Domain की संरचना (Structure)

Active Directory Domain Services (AD DS) एक संरचित और केंद्रीकृत डेटाबेस प्रदान करता है जो नेटवर्क के विभिन्न संसाधनों को प्रबंधित करता है। इसकी संरचना निम्नलिखित घटकों पर आधारित होती है:



मुख्य घटकः

1. **डोमेन (Domain):**

   यह AD DS का मुख्य घटक है, जिसमें सभी यूज़र्स, कंप्यूटर, और संसाधनों की जानकारी संग्रहित होती है। प्रत्येक डोमेन एक सुरक्षा सीमा (security boundary) प्रदान करता है।

2. **ट्री (Tree):**

   एक ट्री एक या अधिक डोमेनों का समूह होता है, जो एक साझा नामकरण स्थान (namespace) के साथ जुड़े होते हैं।

3. **फॉरेस्ट (Forest):**

   फॉरेस्ट AD DS की सबसे बड़ी इकाई होती है, जिसमें एक या अधिक ट्री शामिल हो सकते हैं। यह पूरे नेटवर्क के लिए एक सुरक्षा सीमा और कॉन्फ़िगरेशन प्रदान करता है।

4. **ऑर्गनाइजेशनल यूनिट (OU):**

   OU एक डोमेन के भीतर उप-भाग होते हैं, जिनका उपयोग यूज़र्स, कंप्यूटर, और ग्रुप्स को व्यवस्थित करने के लिए किया जाता है। यह ग्रुप पॉलिसी लागू करने और प्रशासनिक कार्यों को सरल बनाता है।

5. **साइट्स (Sites):**

   साइट्स नेटवर्क टोपोलॉजी पर आधारित है और वे भौगोलिक स्थानों का प्रतिनिधित्व करती है। साइट्स का उपयोग ट्रैफिक प्रबंधन और रेप्लिकेशन के लिए किया जाता है।

3.5 डोमेन कंट्रोलर का उद्देश्य

डोमेन कंट्रोलर (Domain Controller) का मुख्य उद्देश्य नेटवर्क में यूज़र्स और कंप्यूटरों का प्रमाणीकरण (authentication) और अधिकार प्रबंधन (authorization) करना है। यह Active Directory के साथ मिलकर काम करता है और निम्नलिखित कार्य करता हैः

1. प्रमाणीकरणः यह यूज़र्स और डिवाइस की पहचान को सत्यापित करता है ताकि वे सुरक्षित रूप से नेटवर्क संसाधनों तक पहुंच सकें।

2. अधिकार प्रबंधनः डोमेन कंट्रोलर यह सुनिश्चित करता है कि यूज़र्स को उनकी भूमिकाओं के अनुसार उचित संसाधनों तक पहुंच प्रदान की जाए।

SCERT DELHI

3. डाटा रेप्लिकेशनः यह सभी डोमेन कंट्रोलर्स के बीच डेटा का समन्वय (synchronization) करता है ताकि सभी जानकारी अद्यतित (updated) रहे।

3.5.1 डोमेन कंट्रोलर (Domain Controller) के लाभ

डोमेन कंट्रोलर का उपयोग नेटवर्क प्रबंधन और सुरक्षा को सरल और प्रभावी बनाने के लिए किया जाता है। इसके मुख्य लाभ निम्नलिखित हैं:

1. **केंद्रीयकृत प्रबंधन:**

   सभी यूज़र्स, कंप्यूटर और नेटवर्क संसाधनों को एक केंद्रीय स्थान से प्रबंधित किया जा सकता है, जिससे नेटवर्क को आसानी से नियंत्रित किया जा सकता है।

2. **सुरक्षा बढ़ाता है:**

   यह प्रमाणीकरण (authentication) और अधिकृत करना (authorization) सुनिश्चित करता है, जिससे केवल अधिकृत यूज़र्स को ही संसाधनों तक पहुंच मिलती है।

3. **ग्रुप पॉलिसी का कार्यान्वयन:**

   ग्रुप पॉलिसी का उपयोग करके सुरक्षा सेटिंग्स और कॉन्फ़िगरेशन लागू की जा सकती है, जिससे नेटवर्क पर मानकीकरण और सुरक्षा लागू होती है।

4. **डेटा रेप्लिकेशन:**

   सभी डोमेन कंट्रोलर्स के बीच डेटा का स्वचालित रूप से समन्वय (synchronization) होता है, जिससे सभी जानकारी अद्यतित(updated) रहती है।

5. **स्केलेबिलिटी:**

   बड़े नेटवर्क को आसानी से संभाल सकता है और बढ़ती जरूरतों के अनुसार नेटवर्क को विस्तार (scale) किया जा सकता है।

3.5.2 डोमेन कंट्रोलर की सीमाएँ

डोमेन कंट्रोलर का उपयोग नेटवर्क प्रबंधन में सहायक होता है, लेकिन इसकी कुछ सीमाएँ भी हैं:

1. **सिंगल पॉइंट ऑफ फेलियर (Single Point of Failure):**

   यदि केवल एक डोमेन कंट्रोलर होता है और वह विफल हो जाता है, तो नेटवर्क पर यूज़र्स और संसाधनों का प्रमाणीकरण बाधित हो सकता है। इसे हल करने के लिए कई डोमेन कंट्रोलर्स का सेटअप आवश्यक है।

SCERT DELHI

2. जटिलता (Complexity):

बड़े नेटवर्क के लिए डोमेन कंट्रोलर्स को प्रबंधित और कॉन्फ़िगर करना जटिल हो सकता है, खासकर जब कई साइट्स या डोमेन शामिल होते हैं।

3. उच्च संसाधन खपत (High Resource Usage):

डोमेन कंट्रोलर को उचित रूप से काम करने के लिए पर्याप्त हार्डवेयर और नेटवर्क संसाधनों की आवश्यकता होती है, जिससे छोटे संगठनों के लिए इसे प्रबंधित करना चुनौतीपूर्ण हो सकता है।

4. डेटा रेप्लिकेशन की देरी (Replication Delay):

बड़े नेटवर्क में, डोमेन कंट्रोलर्स के बीच डेटा का रेप्लिकेशन धीमा हो सकता है, जिससे जानकारी का अद्यतित (update) होना देरी से होता है।

5. डिपेंडेंसी (Dependency):

अन्य सेवाओं और एप्लिकेशंस का डोमेन कंट्रोलर पर अत्यधिक निर्भर होना, यदि कंट्रोलर विफल हो जाए तो अन्य सेवाओं को भी बाधित कर सकता है।

4. Active Directory Domain Services (AD DS) ऑब्जेक्ट्स का प्रबंधन

4.1 यूज़र अकाउंट्स का प्रबंधन (Managing User Accounts)

उपयोगकर्ता AD में सबसे महत्वपूर्ण वस्तुओं में से एक है। इनका उपयोग प्रमाणीकरण और कार्यस्थानों पर प्राधिकरण के लिए किया जाता है, साथ ही कई सेवाओं में भी जिनका AD के साथ एकीकरण होता है।

सिस्टम एडमिन और हेल्पडेस्क विशेषज्ञों के लिए उपयोगकर्ता प्रबंधन एक मुख्य दिनचर्या है। यह मार्गदर्शिका ऐसे ऑब्जेक्ट्स को कई तरीकों से प्रबंधित करने में मदद करती है।

उपयोगकर्ताओं को प्रबंधित करने के लिए RSAT टूल इंस्टॉल करने या डीसी (डोमेन कंट्रोलर) से सीधे प्रबंधन करने की आवश्यकता होती है।

इसके लिए आपको डोमेन एडमिन या उस अकाउंट से साइन इन होना चाहिए जिसमें वर्तमान OU में ऑब्जेक्ट्स बनाने के लिए ऑपरेटर उपयोगकर्ता या प्रतिनिधिमंडल अधिकार हों।

SCERT DELHI

Active Directory का उपयोग करके यूज़र अकाउंट बनाना (Creating User Account Using Active Directory)

चरण 1: Server Manager खोलें

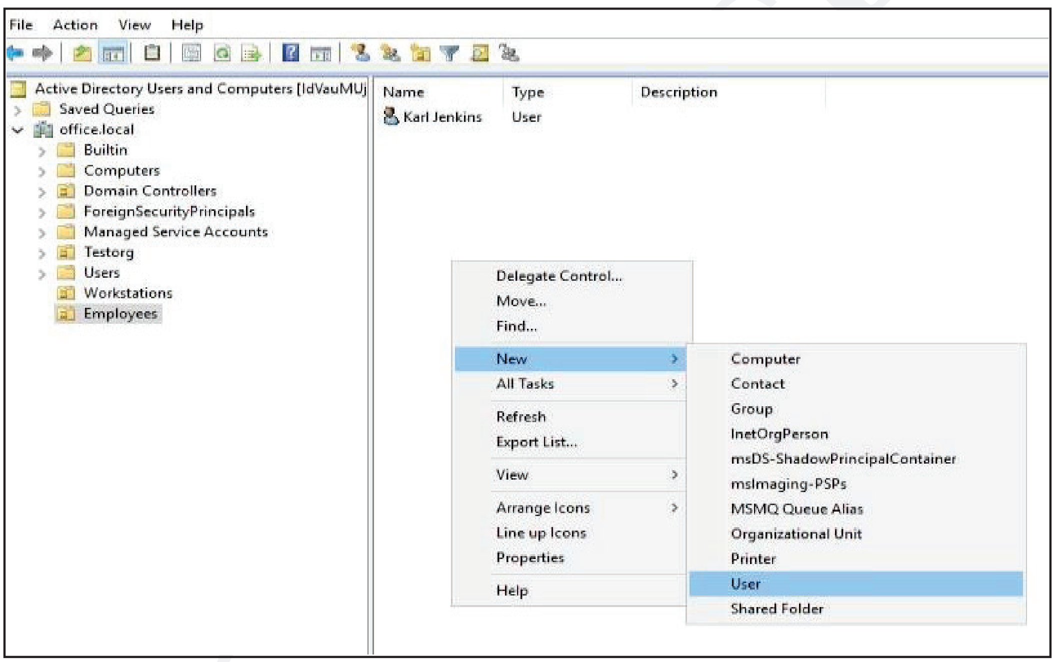
Windows Server में Server Manager खोलें और Active Directory Users and Computers टूल पर नेविगेट करें।

चरण 2: OU का चयन करें

उस Organizational Unit (OU) या कंटेनर का चयन करें जिसमें आप नया यूज़र अकाउंट बनाना चाहते हैं।

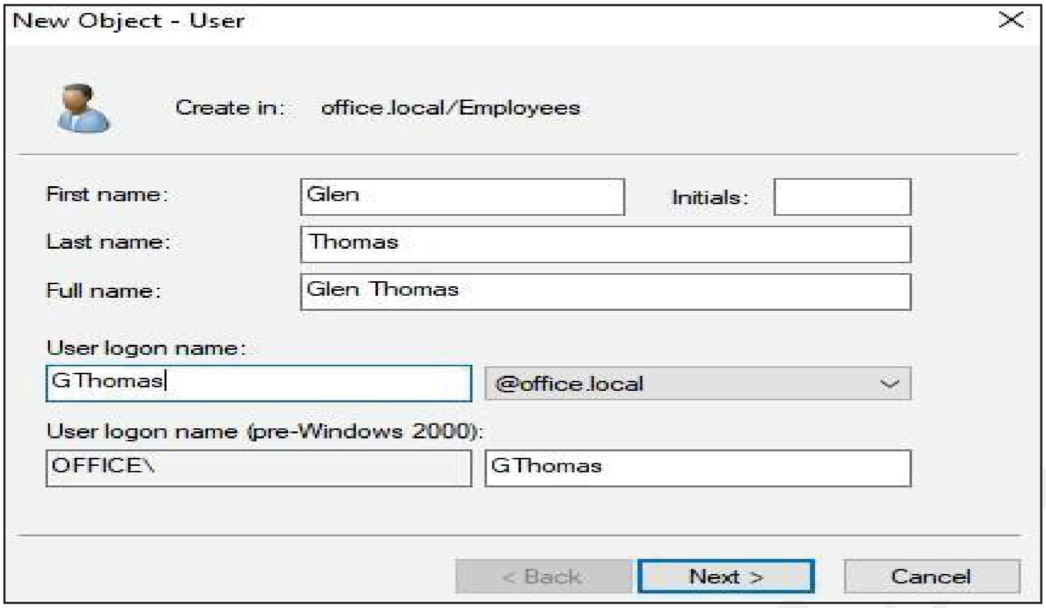
चरण 3: नया यूज़र जोड़ें

OU पर राइट-क्लिक करें, फिर New पर क्लिक करें और User चुनें।



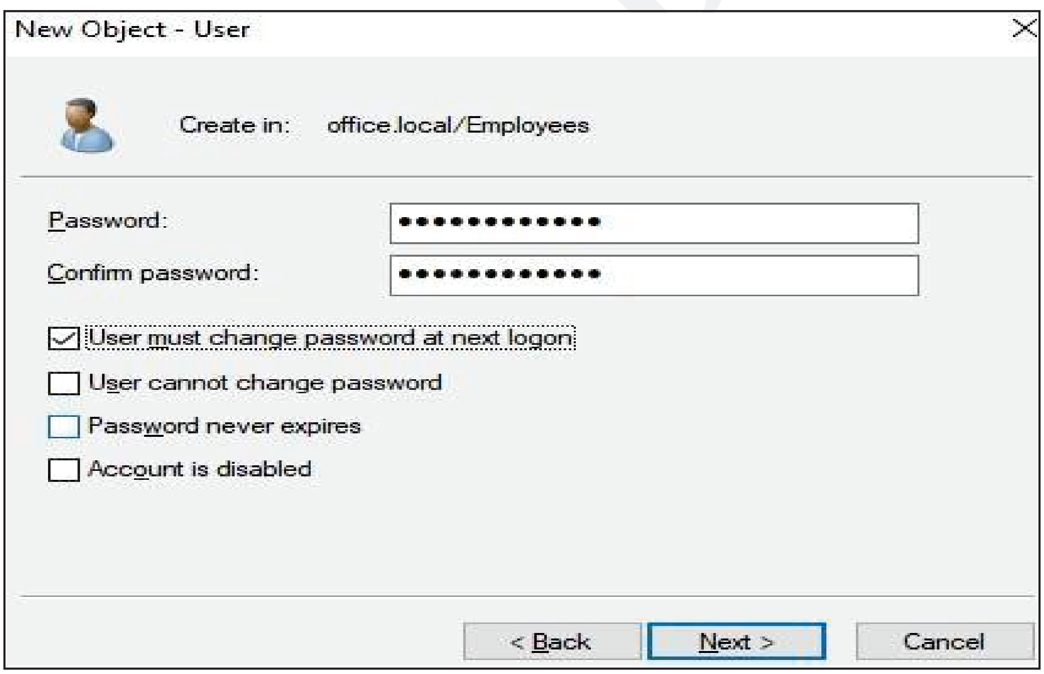
चरण 4: यूज़र जानकारी दर्ज करें

यूज़र का पहला नाम (First Name), अंतिम नाम (Last Name), और लॉगिन नाम (User Logon Name) दर्ज करें।



चरण 5: पासवर्ड सेट करें

यूज़र के लिए पासवर्ड सेट करें और पासवर्ड से संबंधित नीतियाँ चुनें, जैसे कि 'यूज़र को अगले लॉगिन पर पासवर्ड बदलने के लिए मजबूर करना'।



चरण 6: यूज़र अकाउंट पूरा करें

सभी विवरण भरने के बाद Finish पर क्लिक करें। अब नया यूज़र अकाउंट Active Directory में बन चुका है।

कमांड प्रॉम्प्ट का उपयोग करके यूज़र अकाउंट बनाना। (Creating User Account Using Command Prompt)

चरण 1: कमांड प्रॉम्प्ट खोलें

Start मेनू में जाकर Command Prompt को एडमिनिस्ट्रेटर अधिकारों के साथ (Run as Administrator) खोलें।

चरण 2: नई यूज़र अकाउंट बनाने की कमांड दर्ज करें

नया यूज़र अकाउंट बनाने के लिए निम्नलिखित कमांड का उपयोग करें:

net user <username> <password> /add

उदाहरण के लिए, यदि आप john नाम का यूज़र बनाना चाहते हैं और पासवर्ड Password123 सेट करना चाहते हैं, तो कमांड इस प्रकार होगी:

net user john Password123 /add

चरण 3: यूज़र को एडमिनिस्ट्रेटर ग्रुप में जोड़ना (वैकल्पिक)

यदि आप यूज़र को एडमिनिस्ट्रेटर ग्रुप में जोड़ना चाहते हैं, तो निम्नलिखित कमांड का उपयोग करें:

net localgroup administrators <username> /add

उदाहरण के लिए:

net localgroup administrators john /add

चरण 4: यूज़र अकाउंट वेरिफिकेशन

नया यूज़र सफलतापूर्वक बन जाने के बाद, आप इसे सत्यापित करने के लिए निम्नलिखित कमांड का उपयोग कर सकते हैं:

net user <username>

SCERT DELHI

Windows PowerShell का उपयोग करके यूज़र अकाउंट बनाना। (Creating User Account Using Windows PowerShell)

चरण 1: PowerShell खोलें

Start मेनू में जाकर Windows PowerShell को एडमिनिस्ट्रेटर अधिकारों के साथ (Run as Administrator) खोलें।

चरण 2: नया यूज़र अकाउंट बनाने की कमांड

नया यूज़र अकाउंट बनाने के लिए निम्नलिखित कमांड का उपयोग करें:

```
New-LocalUser -Name '<username>' -Password (ConvertTo-SecureString '<password>' -AsPlainText -Force) -FullName '<Full Name>' -Description '<Description>'
```

उदाहरण के लिए, यदि आप john नाम का यूज़र बनाना चाहते हैं, जिसका पासवर्ड Password123 है, तो कमांड इस प्रकार होगी:

```
New-LocalUser -Name 'john' -Password (ConvertTo-SecureString 'Password123' -AsPlainText -Force) -FullName 'John Doe' -Description 'New User Account'
```

चरण 3: यूज़र को ग्रुप में जोड़ना (वैकल्पिक)

यदि आप नए यूज़र को किसी ग्रुप में जोड़ना चाहते हैं, जैसे एडमिनिस्ट्रेटर ग्रुप, तो निम्नलिखित कमांड का उपयोग करें:

```
Add-LocalGroupMember -Group 'Administrators' -Member '<username>'
```

उदाहरण के लिए:

```
Add-LocalGroupMember -Group 'Administrators' -Member 'john'
```

चरण 4: यूज़र अकाउंट वेरिफिकेशन

नया यूज़र सफलतापूर्वक बन जाने के बाद, आप इसे सत्यापित करने के लिए इस कमांड का उपयोग कर सकते हैं:

```
Get-LocalUser
```

SCERT DELHI

यूज़र अकाउंट को डिलीट करने का तरीका

AD वातावरण से यूज़र को डिलीट करें: आसान तरीकों का पालन करते हुए Active Directory (AD) वातावरण से यूज़र को डिलीट करें। ध्यान दें कि यदि AD Recycle Bin सक्षम है, तो यह क्रिया यूज़र अकाउंट को पूरी तरह से डिलीट नहीं करेगी। इसके बजाय, यह यूज़र के टोकन गुणों (token attributes) में बदलाव करेगी और उसे Deleted Objects में स्थानांतरित कर देगी।

आसान तरीके:

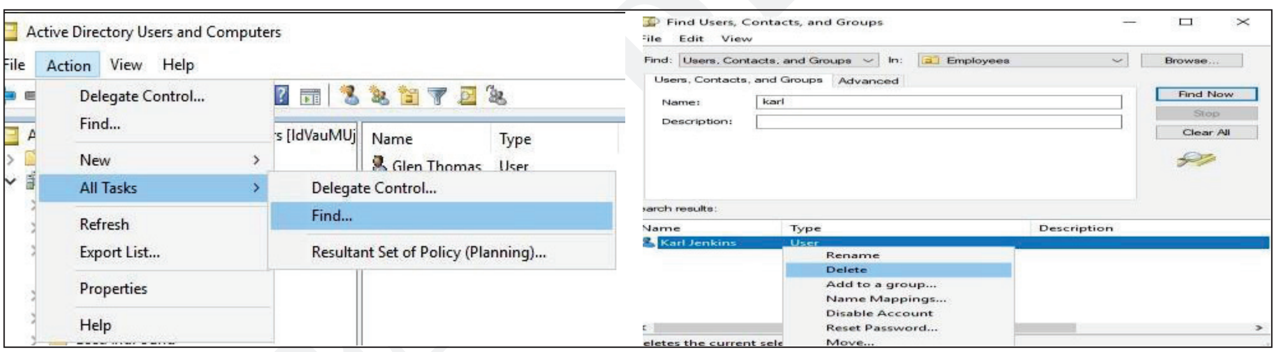
1. **Active Directory Users and Computers (ADUC) का उपयोग करें:**

   ADUC टूल खोलें।

   उस यूज़र को खोजें जिसे आप डिलीट करना चाहते हैं।

   यूज़र पर राइट-क्लिक करें और Delete विकल्प चुनें।

   पुष्टि करें कि आप यूज़र को डिलीट करना चाहते हैं।



2. **PowerShell का उपयोग करें:**

   Windows PowerShell को एडमिनिस्ट्रेटर अधिकारों के साथ खोलें।

   निम्नलिखित कमांड का उपयोग करके यूज़र को डिलीट करें:

   Remove-ADUser -Identity '<username>'

   उदाहरण -

   Remove-ADUser -Identity 'john.doe'

3. **कमांड प्रॉम्प्ट का उपयोग करके यूज़र अकाउंट डिलीट करना (Deleting User Account Using Command Prompt)**

चरण 1: Command Prompt खोलें

Start मेनू से Command Prompt (Run as Administrator) के रूप में खोलें।

चरण 2: यूज़र अकाउंट डिलीट करने की कमांड दर्ज करें

निम्नलिखित कमांड का उपयोग करें:

```
net user <username> /delete
```

उदाहरण के लिए, यदि आप john नाम का यूज़र अकाउंट डिलीट करना चाहते हैं, तो कमांड इस प्रकार होगी:

```
net user john /delete
```

चरण 3: कमांड निष्पादित करें

कमांड दर्ज करने के बाद Enter दबाएं। यह यूज़र अकाउंट को डिलीट कर देगा।

4. **ग्रुप पॉलिसी का कार्यान्वयन (Implementing Group Policy)**

ग्रुप पॉलिसी एक शक्तिशाली टूल है, जो Windows नेटवर्क में यूज़र्स और कंप्यूटरों पर सेटिंग्स और नियम लागू करने के लिए उपयोग किया जाता है। इसके माध्यम से व्यवस्थापक पूरे नेटवर्क पर सुरक्षा और कॉन्फ़िगरेशन सेटिंग्स को केंद्रीकृत तरीके से नियंत्रित कर सकते हैं।

ग्रुप पॉलिसी का कार्यान्वयन:

1. **Group Policy Management Console (GPMC) का उपयोग:**

   Server Manager से Group Policy Management टूल खोलें।

   नई ग्रुप पॉलिसी ऑब्जेक्ट (GPO) बनाने के लिए Create a GPO पर क्लिक करें।

2. **पॉलिसी कॉन्फ़िगरेशन:**

   GPO पर राइट-क्लिक करें और Edit चुनें।

   विभिन्न सेटिंग्स जैसे सिक्योरिटी पॉलिसी, सॉफ़्टवेयर इंस्टॉलेशन, और सिस्टम सेटिंग्स को कॉन्फ़िगर करें।

SCERT DELHI

3. लिंक करना:

नई GPO को किसी ऑर्गनाइजेशनल यूनिट (OU), डोमेन, या साइट से लिंक करें, ताकि वह निर्धारित यूज़र्स या कंप्यूटरों पर लागू हो सके।

4. अपडेट करना:

पॉलिसी को लागू करने के लिए, प्रभावित यूज़र्स और कंप्यूटरों को रिफ्रेश या gpupdate / force कमांड का उपयोग करके अपडेट करें।

ग्रुप पॉलिसी के लाभ:

1. सुरक्षा: पूरे नेटवर्क पर एक समान सुरक्षा नीतियाँ लागू की जा सकती हैं।
2. प्रबंधन: व्यवस्थापक आसानी से कंप्यूटर और यूज़र सेटिंग्स को नियंत्रित कर सकते हैं।
3. प्रभावशीलता: एक ही बार में व्यापक स्तर पर सेटिंग्स और सॉफ़्टवेयर इंस्टॉलेशन लागू करना।

निष्कर्ष:

ग्रुप पॉलिसी नेटवर्क में केंद्रीकृत प्रबंधन के लिए एक महत्वपूर्ण टूल है, जो व्यवस्थापकों को सुरक्षा, कॉन्फ़िगरेशन, और अन्य सेटिंग्स को आसानी से लागू करने की सुविधा प्रदान करता है।

अपनी प्रगति जाँचें

अ. बहु विकल्पीय प्रश्न

1. Windows Server में कौन सा टूल उपयोग किया जाता है सर्वर रोल्स और फीचर्स को जोड़ने के लिए?

a) Control Panel b) Task Manager

c) Server Manager d) Device Manager

2. Windows Server में कौन सी भूमिका (Role) डोमेन कंट्रोलर स्थापित करने के लिए आवश्यक होती है?

a) DHCP

b) DNS

c) Active Directory Domain Services (AD DS)

d) IIS

3. Windows Server पर IP एड्रेस कॉन्फ़िगर करने के लिए निम्नलिखित में से कौन सा विकल्प सही है?

a) Windows Explorer

b) Network and Sharing Center

c) Disk Management

d) Event viewer

4. डिोज सर्वर और नियमित विंडोज़ में मुख्य अंतर क्या है?

a) ग्राफिकल यूजर इंटरफेस   b) उपयोग का उद्देश्य

c) ऑडियो सपोर्ट   d) ब्राउज़र की उपलब्धता

5. Active Directory Domain Services (AD DS) का मुख्य कार्य क्या है?

a) सॉफ़्टवेयर इंस्टॉलेशन   b) यूज़र्स और कंप्यूटरों का प्रबंधन और प्रमाणीकरण

c) डेटा बैकअप   d) नेटवर्क मॉनिटरिंग

6. PowerShell Desired State Configuration (DSC) का मुख्य उद्देश्य क्या है?

a) यूज़र इंटरफेस को कस्टमाइज़ करना   b) नेटवर्क कनेक्टिविटी बढ़ाना

c) कॉन्फ़िगरेशन कोड के रूप में प्रबंधन करना   d) डेटा स्टोरेज बढ़ाना

7. ग्रुप पॉलिसी का कार्यान्वयन करने के लिए कौन सा टूल उपयोग किया जाता है?

a) Task Manager

b) Group Policy Management Console (GPMC)

c) Device Manager

d) Event viewer

SCERT DELHI

8. डोमेन कंट्रोलर की कौन सी विशेषता इसे फॉल्ट टॉलरेंस प्रदान करती है?

a) ग्रुप पॉलिसी
b) मल्टीपल डोमेन कंट्रोलर्स
c) DNS सेटिंग्स
d) यूज़र अकाउंट्स

9. Active Directory में नया यूज़र अकाउंट बनाने के लिए कौन सा कमांड प्रॉम्प्ट में उपयोग किया जाता है?

a) net add user

b) add user

c) net user <username> <password> /add

d) create user <username> <password>

10. Windows Server 2012 में रिमोट डेस्कटॉप सक्षम करने के लिए कौन सा विकल्प चुनना होता है?

a) Control Panel → System

b) Server Manager Local Server Remote Desktop

c) Network and Sharing Center

d) Device Manager Remote Settings

ब. लघु उत्तरीय प्रश्न

1. Windows Server 2012 को प्रबंधित करने के लिए किन प्रमुख टूल्स का उपयोग किया जाता है?

2. स्क्रिप्टिंग भाषा क्या है और इसका क्या उपयोग है?

3. Active Directory Domain Services (AD DS) की स्थापना और कॉन्फ़िगरेशन कैसे की जाती है?

4. डोमेन कंट्रोलर की स्थापना कैसे की जाती है?

5. Active Directory Domain Services (AD DS) ऑब्जेक्ट्स का प्रबंधन कैसे किया जाता है ?

SCERT DELHI

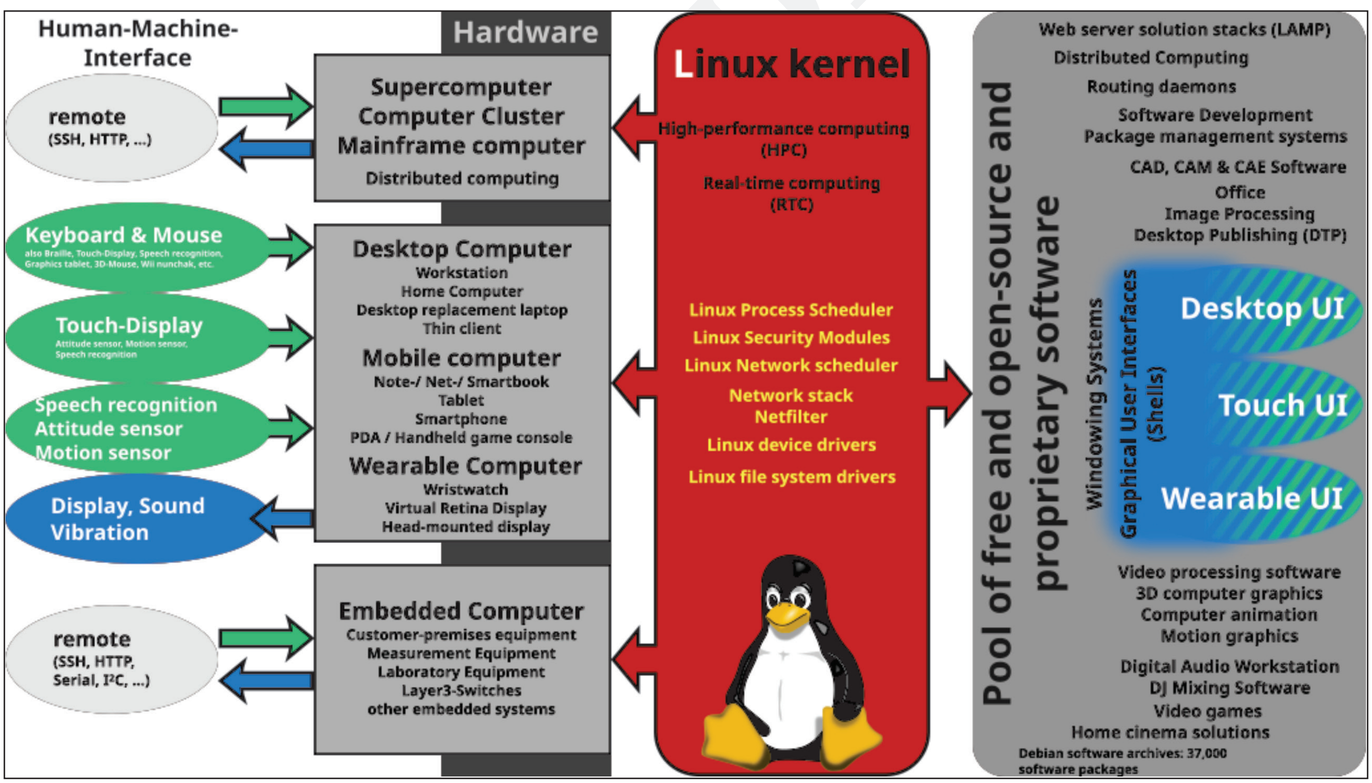
लिनक्स सर्वर की स्थापना और कॉन्फ़िगरेशन

अध्याय 3

परिचय

लिनक्स सर्वर एक ओपन-सोर्स ऑपरेटिंग सिस्टम है, जो विभिन्न प्रकार के सर्वर वातावरणों में इस्तेमाल होता है, जैसे कि वेब सर्वर, फ़ाइल सर्वर, डेटाबेस सर्वर इत्यादि। लिनक्स की विशेषताएँ जैसे इसकी स्थिरता, सुरक्षा, और कस्टमाइज़ेशन की क्षमता इसे बहुत लोकप्रिय बनाती है।

लिनक्स सर्वर की स्थापना और कॉन्फ़िगरेशन की प्रक्रिया विभिन्न चरणों में विभाजित होती है, जिसमें ऑपरेटिंग सिस्टम का चयन, इंस्टॉलेशन, नेटवर्क सेटअप, और आवश्यक सॉफ़्टवेयर पैकेज का इंस्टॉलेशन शामिल होता है। इस प्रक्रिया को सही तरीके से करने से आप एक सुरक्षित और प्रभावी सर्वर तैयार कर सकते हैं।



चित्रः लिनक्स सर्वर विभिन्न प्रकार के हार्डवेयर पर पाया जाता है।

3.1 लिनक्स सर्वर की स्थापना प्रक्रिया

लिनक्स सर्वर की स्थापना एक महत्वपूर्ण प्रक्रिया है जो विभिन्न चरणों में की जाती है। यह प्रक्रिया सुनिश्चित करती है, कि आपका सर्वर सही ढंग से कार्य करे और आवश्यकताओं को पूरा करे। यहां हम इस प्रक्रिया का विस्तृत वर्णन करेंगे।

1. लिनक्स वितरण का चयन करें

लिनक्स के कई वितरण (Distributions) उपलब्ध हैं, जैसेः

* उबंटू सर्वर (Ubuntu Server)
* सेंटओएस (CentOS)
* डेबियन (Debian)
* रेड हैट एंटरप्राइज लिनक्स (आरएचईएल)/(RHEL)

आपकी आवश्यकताओं के अनुसार एक वितरण चुनें और इसकी ISO फ़ाइल आधिकारिक वेबसाइट से डाउनलोड करें।

2. इंस्टॉलेशन मीडिया तैयार करें

लिनक्स सर्वर स्थापित करने के लिए, आपको बूट करने योग्य मीडिया (USB या DvD) बनाना होगा। इसके लिए निम्नलिखित कदम उठाएंः

* **USB ड्राइवः** Rufus (Windows के लिए) या Etcher (क्रॉस-प्लेटफ़ॉर्म) जैसे टूल का उपयोग करके ISO फ़ाइल को USB ड्राइव पर लिखें।
* **DvD:** ISO फ़ाइल को DvD पर बर्न करने के लिए कोई डिस्क-बर्निंग सॉफ़्टवेयर का उपयोग करें।

3. बूट करने के लिए मीडिया डालें

1. USB ड्राइव या DvD को सर्वर में डालें।
2. सर्वर को पॉवर ऑन करें और BIOS/UEFI सेटिंग्स में जाएँ (आमतौर पर बूट के दौरान F2, F10, DEL, या ESC कुंजी दबाकर)।
3. बूट ऑर्डर को USB या DvD से बूट करने के लिए सेट करें।

SCERT DELHI

4. बदलाव सहेजें और BIOS/UEFI सेटिंग्स से बाहर निकलें। अब सर्वर बूट करने के लिए तैयार है।

4. इंस्टॉलेशन प्रक्रिया शुरू करें

बूट करने के बाद, निम्नलिखित चरणों का पालन करें:

1. भाषा और क्षेत्र का चयन करें: अपनी पसंदीदा भाषा और क्षेत्र चुनें।
2. इंस्टॉल करना प्रारंभ करें: 'Install' विकल्प चुनें।
3. डिस्क विभाजन (Disk Partitioning):

 * आप डिस्क को विभाजित कर सकते हैं। आप दो विकल्प चुन सकते हैं:

 स्वचालित विभाजन: इंस्टॉलर इसे अपने आप संभालेगा।

 हस्ताक्षर विभाजन: आप अपने अनुसार विभाजन बना सकते हैं।

 उदाहरण -

 * /(रूट) - ऑपरेटिंग सिस्टम और सॉफ़्टवेयर।
 * /home - उपयोगकर्ता डेटा (वैकल्पिक)।
 * /var - परिवर्तनशील डेटा (जैसे लॉग)।
 * स्वैप - मेमोरी के लिए स्थान।

4. पैकेज चयन (Package Selection):

 आवश्यक सॉफ़्टवेयर पैकेज का चयन करें, जैसे कि:

 * **OpenSSH Server:** दूरस्थ पहुंच के लिए।
 * वेब सर्वर (Apache, Nginx): यदि आप वेब सर्वर सेट करना चाहते हैं।

5. नेटवर्क सेटिंग्स कॉन्फ़िगर करना

1. नेटवर्क कॉन्फ़िगरेशन:

 नेटवर्क सेटिंग्स सेट करें:

* स्थिर IP पता (Static IP Address): एक निश्चित IP पता असाइन करें।
* DHCP: स्वचालित रूप से IP पता प्राप्त करें।

* DNS सर्वर को भी कॉन्फ़िगर करें।

2. होस्ट नाम सेट करें: अपने सर्वर के लिए एक होस्ट नाम सेट करें।

6. उपयोगकर्ता खातों का निर्माण

1. **रूट पासवर्ड सेट करें:** रूट उपयोगकर्ता के लिए एक मजबूत पासवर्ड सेट करें। यह खाता प्रशासनिक विशेषाधिकार रखता है।
2. **गैर-रूट उपयोगकर्ता बनाएं:** एक सामान्य उपयोगकर्ता खाता बनाना बेहतर है, जिसका उपयोग दैनिक कार्यों के लिए किया जाएगा।

7. इंस्टॉलेशन पूरा करें

1. **इंस्टॉलेशन सारांश की समीक्षा करें:** सुनिश्चित करें कि सभी सेटिंग्स सही हैं।
2. **इंस्टॉलेशन प्रारंभ करें:** इंस्टॉलेशन प्रक्रिया शुरू करने के लिए इंस्टॉल बटन पर क्लिक करें। यह कुछ समय ले सकता है।
3. **सर्वर को पुनः बूट करें:** इंस्टॉलेशन पूरा होने पर, सर्वर को पुनः बूट करने के लिए कहा जाएगा।

8. पोस्ट-इंस्टॉलेशन कॉन्फ़िगरेशन

बूट करने के बाद, निम्नलिखित चरण करें:

1. सर्वर में लॉगिन करें: अपने बनाए गए उपयोगकर्ता खाते से लॉगिन करें।
2. सिस्टम अपडेट करें:

* अपने सिस्टम पैकेज को अपडेट करने के लिए निम्नलिखित कमांड चलाएँ:

sudo apt update && sudo apt upgrade	# Ubuntu/Debian के लिए
sudo yum update	# CentOS/RHEL के लिए

SCERT DELHI

3. अतिरिक्त सॉफ़्टवेयर इंस्टॉल करें:

* यदि आवश्यक हो तो कोई अतिरिक्त सॉफ़्टवेयर स्थापित करें:

sudo apt install apache2	# Ubuntu के लिए
sudo yum install httpd	# CentOS के लिए

4. फायरवॉल कॉन्फ़िगर करें:

* सुनिश्चित करें कि फायरवॉल को आवश्यक पोर्ट पर ट्रैफिक अनुमति देने के लिए कॉन्फ़िगर किया गया है।

* उदाहरण के लिए, ufw (Uncomplicated Firewall) का उपयोग करके:

sudo ufw allow 'Apache Full'	# Ubuntu के लिए

5. सेवाएँ सक्षम करें:

* किसी भी आवश्यक सेवा को सक्षम और प्रारंभ करें:

```
sudo systemctl start apache2          # Ubuntu के लिए
sudo systemctl enable apache2         # बूट पर सक्षम करने के लिए
```

3.2 लिनक्स सर्वर प्रबंधन का अवलोकन

लिनक्स सर्वर प्रबंधन का अर्थ है लिनक्स ऑपरेटिंग सिस्टम पर चलने वाले सर्वरों का प्रबंधन और देखभाल करना। यह प्रक्रिया सुनिश्चित करती है कि सर्वर स्थिर, सुरक्षित और प्रभावी ढंग से कार्य कर रहा है। लिनक्स सर्वर प्रबंधन में कई कार्य शामिल होते हैं, जैसे इंस्टॉलेशन, कॉन्फ़िगरेशन, अपडेट, बैकअप और सुरक्षा।

लिनक्स सर्वर प्रबंधन के मुख्य घटक

1. **सर्वर इंस्टॉलेशन:**

* लिनक्स सर्वर का सही तरीके से इंस्टॉलेशन करना।

2. **सर्वर कॉन्फ़िगरेशन:**

* नेटवर्क सेटिंग्स, उपयोगकर्ता खाता निर्माण, और सेवाओं का कॉन्फ़िगरेशन।

3. सर्वर मॉनिटरिंग:

* सर्वर की प्रदर्शन स्थिति की निगरानी करना, जैसे CPU उपयोग, मेमोरी उपयोग, और डिस्क स्पेस।

4. सुरक्षा प्रबंधन:

* फायरवॉल सेटिंग्स, पैच प्रबंधन, और डेटा सुरक्षा उपायों को लागू करना।

5. बैकअप और पुनर्प्राप्ति:

* डेटा और सिस्टम सेटिंग्स का नियमित बैकअप लेना और आपातकालीन स्थितियों में पुनर्प्राप्ति की योजना बनाना।

6. सर्वर अपडेट:

* नए सुरक्षा पैच और सॉफ़्टवेयर अपडेट लागू करना।

लिनक्स सर्वर प्रबंधन की प्रक्रिया

लिनक्स सर्वर प्रबंधन की प्रक्रिया कई चरणों में विभाजित होती है। यह सुनिश्चित करता है कि सर्वर कुशलता से और सुरक्षित रूप से कार्य करे। यहां एक सामान्य प्रक्रिया का वर्णन किया गया है:

1. इंस्टॉलेशन:

* लिनक्स वितरण का चयन करें और सर्वर इंस्टॉलेशन प्रक्रिया का पालन करें।

2. कॉन्फ़िगरेशन:

* सर्वर की बुनियादी सेटिंग्स और नेटवर्क सेटअप करें।

3. सेवाओं का प्रबंधन:

* आवश्यक सेवाओं को स्थापित और कॉन्फ़िगर करें, जैसे वेब सर्वर, डेटाबेस सर्वर आदि।

4. मॉनिटरिंग:

* सर्वर की स्थिति की नियमित रूप से निगरानी करें।

5. सुरक्षा उपाय:

* फायरवॉल और अन्य सुरक्षा उपाय लागू करें।

6. **बैकअप और अपडेट:**

o नियमित बैकअप लें और सर्वर को अपडेट रखें।

लिनक्स सर्वर प्रबंधन का आरेख (Diagram)

```
            ----------------------------
            |     लिनक्स सर्वर        |
            ----------------------------
                        |
      ------------------------------------------
        |           |           |           |
   इंस्टॉलेशन   कॉन्फ़िगरेशन   मॉनिटरिंग   सुरक्षा प्रबंधन
            |           |           |           |
            |           |           |           |
------------------  ------------------  ------------------
| सेवाओं का प्रबंधन |  डेटा बैकअप |  सिस्टम अपडेट  |
------------------  ------------------  ------------------
```

लिनक्स सर्वर प्रबंधन के लाभ

1. **स्थिरता और सुरक्षा:**

* लिनक्स सर्वर बहुत स्थिर होते हैं और उच्च स्तर की सुरक्षा प्रदान करते हैं।

2. **लचीलापन:**

* लिनक्स में विभिन्न प्रकार के सॉफ़्टवेयर और सेवाओं को कस्टमाइज़ करने की क्षमता होती है।

3. **कम लागत:**

* लिनक्स ओपन-सोर्स है, जिससे यह कम लागत में उपलब्ध है।

4. **समर्थन समुदाय:**

* लिनक्स के लिए एक सक्रिय समुदाय है, जो समस्याओं का समाधान प्रदान करता है।

SCERT DELHI

3.3 लिनक्स की फ़ाइल संरचना

लिनक्स ऑपरेटिंग सिस्टम की फ़ाइल संरचना एक विशेष हायरार्किकल सिस्टम में व्यवस्थित होती है। यह संरचना उपयोगकर्ताओं और सिस्टम को फ़ाइलों और डायरेक्टरीज़ को बेहतर तरीके से प्रबंधित करने की अनुमति देती है। फ़ाइल संरचना में मुख्य रूप से रूट डायरेक्टरी (/) और अन्य संबंधित सबडायरेक्टरीज़ शामिल होती हैं।

लिनक्स फ़ाइल संरचना का अवलोकन

लिनक्स में फ़ाइल संरचना को रूट डायरेक्टरी (/) से शुरू किया जाता है। इस रूट डायरेक्टरी के अंतर्गत विभिन्न सबडायरेक्टरीज़ होती हैं जो विशेष कार्यों और फ़ाइलों को संग्रहित करती हैं। यहाँ पर कुछ महत्वपूर्ण डायरेक्टरीज़ का विवरण दिया गया है:

1. **/ (रूट डायरेक्टरी):**
   * यह लिनक्स फ़ाइल प्रणाली की आधारभूत डायरेक्टरी है।

2. **/bin:**
   * इस डायरेक्टरी में बुनियादी उपयोगकर्ता कमांड्स और प्रोग्राम्स होते हैं, जैसे ls, cp, mv आदि।

3. **/boot:**
   * इस डायरेक्टरी में बूट करने के लिए आवश्यक फाइलें होती हैं, जैसे कि कर्नेल और ग्रब।

4. **/etc:**
   * सिस्टम की कॉन्फ़िगरेशन फ़ाइलें यहाँ स्थित होती हैं। उदाहरण के लिए, passwd, fstab, आदि।

5. **/home:**
   * प्रत्येक उपयोगकर्ता के व्यक्तिगत फ़ाइलों और सेटिंग्स का भंडारण। प्रत्येक उपयोगकर्ता के लिए एक सबडायरेक्टरी होती है, जैसे /home/username।

6. **/lib:**
   * सिस्टम लाइब्रेरी फाइलें जो बाइनरी प्रोग्राम्स द्वारा उपयोग की जाती हैं।

SCERT DELHI

7. /media:

* यहाँ पर removable devices (जैसे USB ड्राइव) को माउंट किया जाता है।

8. /opt:

* वैकल्पिक एप्लिकेशन्स और पैकेजेस के लिए यहाँ स्थान होता है।

9. /root:

* यह रूट उपयोगकर्ता (administrative user) की व्यक्तिगत डायरेक्टरी है।

10. /sbin:

* सिस्टम प्रशासनिक कमांड्स यहाँ होते हैं, जैसे कि shutdown, reboot आदि।

11. /tmp:

* अस्थायी फ़ाइलों के लिए डायरेक्टरी। यह आमतौर पर बूट के दौरान साफ की जाती है।

12. /usr:

* यहाँ पर उपयोगकर्ता स्तर के प्रोग्राम और फाइलें होती हैं, जैसे कि /usr/bin और /usr/lib।

13. /var:

* यह डायरेक्टरी परिवर्तनशील डेटा जैसे कि लॉग फ़ाइलें और स्पूल फ़ाइलें रखती है।

लिनक्स फ़ाइल संरचना का आरेख (Diagram)

```
/
├── bin
├── boot
├── etc
├── home
│   ├── user1
│   └── user2
├── lib
├── media
├── opt
├── root
├── sbin
├── tmp
├── usr
└── var
```

SCERT DELHI

लिनक्स फ़ाइल संरचना के लाभ

1. संगठितः

* फ़ाइलों और डायरेक्टरीज़ का स्पष्ट विभाजन सिस्टम को अधिक संगठित बनाता है।

2. सुरक्षाः

* विभिन्न उपयोगकर्ताओं के लिए अलग-अलग डायरेक्टरीज़ सुरक्षा को बढ़ाती हैं।

3. प्रवेश सरलताः

* उपयोगकर्ता आसानी से अपने फ़ाइलों और सेटिंग्स तक पहुँच सकते हैं।

4. प्रबंधन में आसानीः

* सिस्टम प्रशासक के लिए फ़ाइलों और डायरेक्टरीज़ का प्रबंधन करना आसान होता है।

3.4 लिनक्स फ़ाइल संरचना के प्रकार

लिनक्स फ़ाइल संरचना एक विशेष हायरार्किकल (Hierarchical) मॉडल पर आधारित होती है, जिसमें विभिन्न प्रकार की फ़ाइलें और डायरेक्टरीज़ होती हैं। यह प्रणाली उपयोगकर्ताओं को फ़ाइलों और डेटा को व्यवस्थित करने और प्रबंधित करने में मदद करती है। लिनक्स में फ़ाइलों की संरचना को मुख्यतः तीन प्रकारों में वर्गीकृत किया जा सकता हैः

1. **फाइल डायरेक्टरी (File Directory)**
2. **स्पेशल फ़ाइलें (Special Files)**
3. **डिवाइस फ़ाइलें (Device Files)**

1. फ़ाइल डायरेक्टरी (File Directory)

परिभाषाः यह सामान्य फ़ाइलें हैं, जो उपयोगकर्ता द्वारा बनाई जाती हैं या सिस्टम द्वारा उत्पन्न होती हैं। इनमें टेक्स्ट फ़ाइलें, बाइनरी फ़ाइलें, इमेज फ़ाइलें आदि शामिल होती हैं।

उदाहरण –

* /home/user/Documents/: उपयोगकर्ता के दस्तावेज़
* /home/user/Music/: उपयोगकर्ता की संगीत फ़ाइलें

SCERT DELHI

2. स्पेशल फ़ाइलें (Special Files)

परिभाषा: ये फ़ाइलें विशेष कार्य करती हैं, जैसे कि डेटा को स्टोर करना, प्रोसेस से संवाद करना आदि। इन्हें अक्सर कर्नेल द्वारा प्रबंधित किया जाता है।

प्रकार:

* **FIFO (First In First Out):** इनका उपयोग डेटा के प्रवाह को नियंत्रित करने के लिए किया जाता है।
* **Sockets:** नेटवर्क कम्युनिकेशन के लिए।

उदाहरण –

* **/dev/null:** एक विशेष फ़ाइल जो सभी डेटा को हटा देती है।
* **/dev/tty:** टर्मिनल इंटरफेस के लिए।

3. डिवाइस फ़ाइलें (Device Files)

परिभाषा: ये फ़ाइलें हार्डवेयर उपकरणों के लिए होती हैं, जो उपयोगकर्ता को उपकरणों के साथ इंटरैक्ट करने की अनुमति देती हैं।

प्रकार:

* ब्लॉक डिवाइस फ़ाइलें: ये फ़ाइलें डेटा को ब्लॉक्स में पढ़ती और लिखती हैं, जैसे हार्ड डिस्क।
* चर डिवाइस फ़ाइलें: ये फ़ाइलें डेटा को एक समय में एक बाइट में पढ़ती और लिखती हैं, जैसे की कीबोर्ड या माउस।

उदाहरण –

* **/dev/sda:** पहला हार्ड डिस्क ड्राइव।
* **/dev/ttyS0:** पहला सीरियल पोर्ट।

SCERT DELHI

लिनक्स फ़ाइल संरचना का आरेख (Diagram)

```
/
├── File Types
│   ├── Regular Files
│   │   ├── /home/user/Documents
│   │   └── /home/user/Music
│   ├── Special Files
│   │   ├── FIFO
│   │   ├── Sockets
│   │   └── /dev/null
│   └── Device Files
│       ├── Block Devices
│       │   └── /dev/sda
│       └── Character Devices
│           └── /dev/ttyS0
└── Other Directories
```

3.5 सेवाओं के लिए पैकेज इंस्टॉल करना और हटाना

लिनक्स में पैकेज मैनेजमेंट एक महत्वपूर्ण प्रक्रिया है जो उपयोगकर्ताओं को सॉफ़्टवेयर और सेवाओं को इंस्टॉल, अपडेट और हटाने की अनुमति देती है। विभिन्न लिनक्स वितरण में पैकेज प्रबंधन के लिए अलग-अलग टूल होते हैं, जैसे कि apt (डेबियन और उबंटू), yum (रेड हैट, सेंटओएस) और dnf (फेडोरा)।

पैकेज इंस्टॉल करना

उदाहरण - apt का उपयोग करके पैकेज इंस्टॉल करना (उबंटू)

1. **टर्मिनल खोलें।**
2. **अपडेट करें:**

```
sudo apt update
```

3. **पैकेज इंस्टॉल करें:**

```
sudo apt install package-name
```

*   यहाँ package-name उस पैकेज का नाम है जिसे आप इंस्टॉल करना चाहते हैं।

उदाहरण - yum का उपयोग करके पैकेज इंस्टॉल करना (रेड हैट)

SCERT DELHI

1. टर्मिनल खोलें।
2. पैकेज इंस्टॉल करें:

```
sudo yum install package-name
```

पैकेज हटाना

उदाहरण - apt का उपयोग करके पैकेज हटाना (उबंटू)

1. टर्मिनल खोलें।
2. पैकेज हटाने के लिए:

```
sudo apt remove package-name
```

उदाहरण - yum का उपयोग करके पैकेज हटाना (रेड हैट)

1. टर्मिनल खोलें।
2. पैकेज हटाने के लिए:

```
sudo yum remove package-name
```

पैकेज इंस्टॉलेशन और हटाने की प्रक्रिया का आरेख (Diagram)

```
                 |     टर्मिनल     |
                 ------------------
                         |
                         |
         ------------------------------------
         |                                  |
   पैकेज इंस्टॉल करना                      पैकेज हटाना
         |                                  |
         |                                  |
------------------                  ------------------
|    अपडेट करें    |                  |    हटाएं पैकेज    |
|  sudo apt update |                    | sudo apt remove  |
|  sudo yum update  |                    | sudo yum remove   |
------------------                  ------------------
         |                                  |
         |                                  |
------------------                  ------------------
| इंस्टॉल पैकेज     |                 | हटाए गए पैकेज    |
| sudo apt install|                   | sudo apt remove   |
| sudo yum install |                    | sudo yum remove   |
------------------                  ------------------
```

SCERT DELHI

अपनी प्रगति जाँचें

अ. बहु विकल्पीय प्रश्न

1. **लिनक्स सर्वर की स्थापना के लिए सबसे पहले कौन सा कदम उठाया जाता है?**

   A. फाइल सिस्टम को सेटअप करना

   B. ऑपरेटिंग सिस्टम की ISO फ़ाइल डाउनलोड करना

   C. नेटवर्क सेटिंग्स को कॉन्फ़िगर करना

   D. उपयोगकर्ता खातों को बनाना

2. **लिनक्स सर्वर प्रबंधन में कौन सा उपकरण सामान्यतः उपयोग किया जाता है?**

   A. Microsoft Word   B. PuTTY

   C. Adobe Photoshop   D. vLC Media Player

3. **लिनक्स की फ़ाइल संरचना का मूल तत्व क्या है?**

   A. /etc   B. /bin

   C. /home   D. /root

4. **लिनक्स फ़ाइल संरचना के प्रकार में निम्नलिखित में से कौन सा शामिल नहीं है?**

   A. एब्सोल्यूट पाथ   B. रिलेटिव पाथ

   C. संदर्भ पाथ   D. हार्ड लिंक

5. **लिनक्स सर्वर पर पैकेज इंस्टॉल करने के लिए कौन सा कमांड आमतौर पर उपयोग किया जाता** है?

   A. installpkg   B. apt-get install

   C. setuppkg   D. addpkg

6. **लिनक्स सर्वर से पैकेज हटाने के लिए कौन सा कमांड उपयोग किया जाता है?**

   A. removepkg   B. apt-get remove

   C. delpkg   D. uninstpkg

SCERT DELHI

7. **लिनक्स फ़ाइल संरचना में '/home' डायरेक्टरी का क्या कार्य है?**

A. सिस्टम फ़ाइलें संग्रहीत करना

B. उपयोगकर्ता की व्यक्तिगत फ़ाइलें संग्रहीत करना

C. प्रोग्राम फ़ाइलें संग्रहीत करना

D. सिस्टम लॉग फ़ाइलें संग्रहीत करना

8. **लिनक्स में सर्वर प्रबंधन का कौन सा हिस्सा महत्वपूर्ण है?**

A. केवल सिस्टम अपडेट

B. उपयोगकर्ता प्रबंधन, सुरक्षा, और सेवाओं की निगरानी

C. केवल बैकअप लेना

D. केवल नेटवर्क सेटिंग्स बदलना

9. **लिनक्स सर्वर पर कौन सी सेवा आमतौर पर चलती है?**

A. FTP

B. HTTP

C. SSH

D. उपरोक्त सभी

10. **लिनक्स फ़ाइल संरचना में 'root' यूज़र का क्या महत्व है?**

A. यह सबसे सामान्य उपयोगकर्ता होता है

B. यह सिस्टम के लिए सभी अधिकारों के साथ एक सुपरयूजर होता है

C. यह केवल फ़ाइलें देख सकता है

D. यह केवल नेटवर्क सेटिंग्स को बदल सकता है

SCERT DELHI

ब. लघु उत्तरीय प्रश्न

1. लिनक्स सर्वर की स्थापना प्रक्रिया में पहले चरण के रूप में क्या करना चाहिए?
2. लिनक्स सर्वर प्रबंधन का प्रमुख उद्देश्य क्या है?
3. लिनक्स की फ़ाइल संरचना में कौन सी डायरेक्टरी उपयोगकर्ता की व्यक्तिगत फ़ाइलों के लिए होती है?
4. लिनक्स में पैकेज इंस्टॉल करने के लिए कौन सा कमांड सामान्यतः उपयोग किया जाता है?
5. लिनक्स फ़ाइल संरचना के प्रकारों में से कौन सा पथ विशेष रूप से एक फ़ाइल या डायरेक्टरी को निर्दिष्ट करता है?

❖❖❖

SCERT DELHI

आईटी सुरक्षा के बुनियादी सिद्धांत

अध्याय 4

परिचय

आईटी (सूचना प्रौद्योगिकी) सुरक्षा आज के डिजिटल युग में एक महत्वपूर्ण विषय है। यह उन प्रक्रियाओं, नीतियों, और उपायों का समूह है जो कंप्यूटर सिस्टम, नेटवर्क, और डेटा को सुरक्षा खतरों से सुरक्षित रखने के लिए उपयोग किया जाता है। हर व्यक्ति या संगठन जो इंटरनेट या किसी भी प्रकार की तकनीक का उपयोग करता है, उन्हें आईटी सुरक्षा की बुनियादी समझ होनी चाहिए, ताकि साइबर खतरों से बचा जा सके।

4.1 आईटी सुरक्षा के सिद्धांत

आईटी सुरक्षा, या सूचना प्रौद्योगिकी सुरक्षा, आज की डिजिटल दुनिया में एक आवश्यक आवश्यकता है। यह संगठनों और व्यक्तिगत उपयोगकर्ताओं के लिए डेटा की सुरक्षा, गोपनीयता, और नेटवर्क की अखंडता को सुनिश्चित करता है। आईटी सुरक्षा की अवधारणा में तकनीकी और प्रबंधन उपाय शामिल होते हैं, जो सूचना प्रणाली को सुरक्षा खतरों से बचाने में मदद करते हैं।

आईटी सुरक्षा के मुख्य सिद्धांत

आईटी सुरक्षा के सिद्धांतों को आमतौर पर तीन मुख्य घटकों के रूप में जाना जाता है, जिन्हें CIA ट्रायएड के नाम से जाना जाता है:

1. **गोपनीयता (Confidentiality):**
   - यह सुनिश्चित करता है, कि संवेदनशील जानकारी केवल अधिकृत व्यक्तियों के लिए उपलब्ध हो।
   - डेटा एन्क्रिप्शन और एक्सेस कंट्रोल द्वारा इसे सुनिश्चित किया जाता है।

2. **अखंडता (Integrity):**
   - यह डेटा की सटीकता और पूर्णता को बनाए रखने का सिद्धांत है।
   - किसी भी अनधिकृत बदलाव को रोकने के लिए चेकसम और हैशिंग तकनीकों का उपयोग किया जाता है।

SCERT DELHI

3. उपलब्धता (Availability):

* यह सुनिश्चित करता है कि डेटा और संसाधन उपयोगकर्ताओं के लिए हमेशा उपलब्ध हों।
* सिस्टम की निरंतरता सुनिश्चित करने के लिए बैकअप और आपातकालीन योजना का पालन किया जाता है।

आईटी सुरक्षा के प्रमुख खतरे

आईटी सुरक्षा के क्षेत्र में निम्नलिखित प्रमुख खतरे होते हैं:

1. वायरस और मालवेयर:

* ये कंप्यूटर में घुसकर डेटा को नष्ट कर सकते हैं या चोरी कर सकते हैं।

2. हैकिंग:

* अनधिकृत उपयोगकर्ता सिस्टम में घुसपैठ कर सकते हैं।

3. फिशिंग:

* धोखाधड़ी के माध्यम से उपयोगकर्ताओं की संवेदनशील जानकारी चुराने का प्रयास।

4. डी-डीओएस अटैक (DDoS):

* यह हमला सर्वर को ठप करने के लिए भारी मात्रा में ट्रैफिक भेजकर किया जाता है।

आईटी सुरक्षा के उपाय

आईटी सुरक्षा को सुनिश्चित करने के लिए निम्नलिखित उपाय किए जा सकते हैं:

1. फायरवॉल:

* नेटवर्क सुरक्षा का प्राथमिक उपाय है जो अवांछित ट्रैफिक को रोकता है।

2. एंटीवायरस सॉफ़्टवेयर:

* यह आपके सिस्टम को वायरस और मालवेयर से सुरक्षित रखता है।

3. सुरक्षित पासवर्ड प्रथाएँ:

* मजबूत और अद्वितीय पासवर्ड का उपयोग करना।

SCERT DELHI

4. डेटा एन्क्रिप्शनः

* संवेदनशील डेटा को सुरक्षित करने के लिए एन्क्रिप्ट किया जाता है।

5. बैकअपः

* नियमित रूप से डेटा का बैकअप लेना।

आईटी सुरक्षा का आरेख (Diagram)

```
                                आईटी सुरक्षा
                                     |
        ----------------------------------------------------------
        |                            |                            |
गोपनीयता (C)              अखंडता (I)              उपलब्धता (A)
        |                            |                            |
डेटा एन्क्रिप्शन           चेकसम/हैशिंग          बैकअप/रिप्लेसमेंट
        |                            |                            |
एक्सेस नियंत्रण             डेटा सुरक्षा             फॉल्ट टॉलरेंस
        |
उपयोगकर्ता प्रमाणीकरण
```

4.2 एंटीवायरस सॉफ्टवेयर का उपयोग

एंटीवायरस सॉफ्टवेयर एक प्रकार का प्रोग्राम है जो कंप्यूटर सिस्टम को वायरस, मालवेयर, और अन्य साइबर खतरों से सुरक्षित रखने के लिए डिज़ाइन किया गया है। यह सॉफ्टवेयर सिस्टम की सुरक्षा सुनिश्चित करने में महत्वपूर्ण भूमिका निभाता है। एंटीवायरस सॉफ्टवेयर न केवल वायरस को पहचानता है, बल्कि इसे हटाने और सुरक्षा उपायों के सुझाव देने में भी मदद करता है।

एंटीवायरस सॉफ्टवेयर के कार्य

1. स्कैनिंग (Scanning):

* एंटीवायरस सॉफ्टवेयर नियमित रूप से सिस्टम के फ़ाइलों और प्रोग्रामों को स्कैन करता है, ताकि किसी भी संभावित खतरे को पहचान सके।

2. वायरस पहचानना (virus Detection):

* यह ज्ञात वायरस की पहचान करने के लिए सिग्नेचर-आधारित और हीयूरिस्टिक तकनीकों का उपयोग करता है।

3. वायरस को हटाना (virus Removal):

* यदि कोई वायरस या मालवेयर पहचान लिया जाता है, तो एंटीवायरस उसे हटाने या क्वारंटाइन करने की प्रक्रिया शुरू करता है।

4. रियल-टाइम सुरक्षा (Real-time Protection):

* यह सॉफ्टवेयर लगातार कंप्यूटर पर नज़र रखता है और संदिग्ध गतिविधियों की तुरंत पहचान करता है।

5. सिस्टम अपडेट (System Updates):

* एंटीवायरस सॉफ्टवेयर को समय-समय पर अपडेट किया जाता है, ताकि यह नवीनतम वायरस से सुरक्षित रह सके।

एंटीवायरस सॉफ़्टवेयर का उपयोग कैसे करें

1. इंस्टॉलेशन (Installation):

* सबसे पहले, एंटीवायरस सॉफ्टवेयर को डाउनलोड और इंस्टॉल करें।

* उदाहरण - Norton, McAfee, Avast, Kaspersky आदि।

2. पहली स्कैनिंग (Initial Scanning):

* इंस्टॉलेशन के बाद, एंटीवायरस सॉफ्टवेयर को पहली बार कंप्यूटर की पूरी स्कैनिंग करने दें।

3. नियमित स्कैनिंग (Regular Scanning):

* सेटिंग्स में जाकर शेड्यूल्ड स्कैनिंग का चयन करें ताकि यह नियमित अंतराल पर स्कैन करता रहे।

4. रियल-टाइम प्रोटेक्शन चालू करें (Enable Real-time Protection):

* सुनिश्चित करें कि रियल-टाइम प्रोटेक्शन सक्षम है ताकि संदिग्ध गतिविधियों पर तुरंत कार्रवाई की जा सके।

5. नवीनतम अपडेट (Keep Updated):

* एंटीवायरस सॉफ्टवेयर को हमेशा नवीनतम अपडेट रखने का प्रयास करें।

SCERT DELHI

एंटीवायरस सॉफ्टवेयर के उपयोग का आरेख (Diagram)

```
                  एंटीवायरस सॉफ़्टवेयर का उपयोग
                               |
           -----------------------------------
           |                   |                  |
      इंस्टॉलेशन          स्कैनिंग            अपडेट करना
           |                   |                  |
  डाउनलोड और इंस्टॉल     पूरी स्कैनिंग      नवीनतम वायरस सिग्नेचर
           |                   |                  |
           |                   |                  |
           |                   |                  |
    रियल-टाइम प्रोटेक्शन    पहचानना और हटाना
           |                   |
   संदिग्ध गतिविधि का      संक्रमित फ़ाइलें हटाना
       पता लगाना
```

4.3 कमज़ोरियों (vulnerabilities) का वर्णन

कमज़ोरियाँ (vulnerabilities) किसी सिस्टम, नेटवर्क, या एप्लिकेशन में वो खामियाँ होती हैं जो साइबर हमलों का शिकार बन सकती हैं। ये कमज़ोरियाँ विभिन्न कारणों से हो सकती हैं, जैसे कि सॉफ्टवेयर बग्स, खराब कॉन्फ़िगरेशन, या सुरक्षा नीतियों की कमी। कमज़ोरियों का पता लगाना और उन्हें सुधारना किसी भी सुरक्षा योजना का महत्वपूर्ण हिस्सा है।

कमज़ोरियों के प्रकार

1. **सॉफ्टवेयर कमज़ोरियाँ (Software vulnerabilities):**

   * सॉफ्टवेयर में बग्स या कोड में त्रुटियाँ होती हैं जो उसे हमले के लिए असुरक्षित बना सकती हैं। उदाहरण - SQL इंजेक्शन, क्रॉस-साइट स्क्रिप्टिंग (XSS)।

2. **नेटवर्क कमज़ोरियाँ (Network vulnerabilities):**

   * नेटवर्क सुरक्षा में कमी या असुरक्षित नेटवर्क प्रोटोकॉल जो डेटा की चोरी का कारण बन सकते हैं। उदाहरण - खुला वाई-फाई नेटवर्क, बिना फायरवॉल के नेटवर्क।

3. **हार्डवेयर कमज़ोरियाँ (Hardware vulnerabilities):**

   * हार्डवेयर में कमजोरियां, जैसे कि फिजिकल एक्सेस का अभाव। उदाहरण - असुरक्षित सर्वर रूम।

SCERT DELHI

4. मानव कारक (Human Factors):

- मानव त्रुटियां या अनजाने में सुरक्षा नीतियों की अनदेखी। उदाहरण - कमजोर पासवर्ड का उपयोग, फ़िशिंग अटैक्स का शिकार होना।

कमज़ोरियों के प्रभाव

डेटा चोरी: संवेदनशील डेटा का चोरी होना।

सिस्टम ठप होना: सिस्टम या नेटवर्क का ठप होना।

वित्तीय नुकसान: साइबर हमलों के कारण आर्थिक नुकसान।

विश्वसनीयता की हानि: ग्राहकों और उपयोगकर्ताओं के प्रति विश्वसनीयता की कमी।

कमज़ोरियों का आरेख (Diagram)

```
                    कमज़ोरियाँ (Vulnerabilities)
                                 |
          ----------------------------------------
          |                      |                    |
   सॉफ़्टवेयर                  नेटवर्क               हार्डवेयर
   कमज़ोरियाँ                  कमज़ोरियाँ            कमज़ोरियाँ
          |                      |                    |
-----------------    -----------------    -----------------
|   बग्स/त्रुटियाँ |    खुला वाई-फाई    |    असुरक्षित सर्वर
|   (SQL, XSS)     |   बिना फायरवॉल    |     रूम
-----------------    -----------------    -----------------
                                 |
                            मानव कारक
                                 |
                     ---------------------
                     |                   |
              कमजोर पासवर्ड          फ़िशिंग अटैक
```

4.4 सुरक्षा प्रक्रियाएँ (Security Procedures)

सुरक्षा प्रक्रियाएँ उन नियमों और उपायों का सेट हैं जिन्हें किसी संगठन या प्रणाली की सुरक्षा सुनिश्चित करने के लिए लागू किया जाता है। ये प्रक्रियाएँ किसी भी संभावित खतरे से बचाव करने, डेटा की

सुरक्षा करने, और संगठनों की परिसंपत्तियों की सुरक्षा में मदद करती हैं। सुरक्षा प्रक्रियाएँ तकनीकी और प्रबंधन दोनों उपायों का संयोजन हो सकती हैं।

सुरक्षा प्रक्रियाओं के प्रमुख घटक

1. उपयोगकर्ता प्रमाणीकरण (User Authentication):

* यह प्रक्रिया सुनिश्चित करती है कि केवल अधिकृत उपयोगकर्ताओं को ही सिस्टम या डेटा तक पहुँच प्राप्त हो। आमतौर पर उपयोगकर्ता नाम और पासवर्ड का उपयोग किया जाता है।

2. एक्सेस नियंत्रण (Access Control):

* यह निर्धारित करता है कि किस उपयोगकर्ता को कौन सी जानकारी या संसाधनों तक पहुँच प्राप्त है। इसमें RBAC (Role-Based Access Control) और ACL (Access Control List) शामिल हैं।

3. डेटा एन्क्रिप्शन (Data Encryption):

* संवेदनशील डेटा को एन्क्रिप्ट किया जाता है ताकि इसे बिना अनुमति के न पढ़ा जा सके। यह डेटा की गोपनीयता सुनिश्चित करता है।

4. फायरवॉल और नेटवर्क सुरक्षा (Firewall and Network Security):

* फायरवॉल का उपयोग अवांछित ट्रैफिक को रोकने और नेटवर्क को सुरक्षित रखने के लिए किया जाता है।

5. नियमित सुरक्षा परीक्षण (Regular Security Testing):

* सिस्टम की सुरक्षा को जांचने के लिए नियमित रूप से सुरक्षा परीक्षण (penetration testing) और ऑडिट किए जाते हैं।

6. सुरक्षा जागरूकता और प्रशिक्षण (Security Awareness and Training):

* कर्मचारियों को सुरक्षा नीतियों और प्रक्रियाओं के बारे में प्रशिक्षित किया जाता है ताकि वे संभावित खतरों से जागरूक रह सकें।

सुरक्षा प्रक्रियाओं का आरेख (Diagram)

```
                    सुरक्षा प्रक्रियाएँ (Security Procedures)
                                      |
        ---------------------------------------------------------------
        |                 |                 |                 |           |
उपयोगकर्ता प्रमाणीकरण   एक्सेस नियंत्रण   डेटा एन्क्रिप्शन   फायरवॉल   नियमित सुरक्षा परीक्षण
        |                 |                 |                 |           |
  उपयोगकर्ता नाम और     RBAC / ACL      संवेदनशील डेटा     नेटवर्क    पेनिट्रेशन टेस्टिंग
      पासवर्ड             |             एन्क्रिप्टेड        सुरक्षा       और ऑडिट
                            |
              उपयोगकर्ता समूहों
```

4.5 सुरक्षित डेटा (Protected Data) का वर्णन

सुरक्षित डेटा (Protected Data) वह डेटा होता है जिसे अनधिकृत पहुँच, चोरी, या क्षति से बचाने के लिए विभिन्न सुरक्षा उपायों और तकनीकों का उपयोग करके सुरक्षित किया जाता है। इस डेटा में संवेदनशील जानकारी हो सकती है, जैसे कि व्यक्तिगत जानकारी, वित्तीय डेटा, या किसी संगठन की व्यावसायिक जानकारी। डेटा सुरक्षा सुनिश्चित करने के लिए संगठनों को विभिन्न नीतियों और प्रक्रियाओं का पालन करना होता है।

सुरक्षित डेटा के प्रकार

1. **व्यक्तिगत डेटा (Personal Data):**
   * नाम, पता, ईमेल, फ़ोन नंबर आदि जैसे व्यक्तिगत पहचान योग्य जानकारी।
2. **वित्तीय डेटा (Financial Data):**
   * बैंक खाता जानकारी, क्रेडिट कार्ड विवरण, और लेनदेन की जानकारी।
3. **स्वास्थ्य डेटा (Health Data):**
   * चिकित्सा इतिहास, रोगी रिकॉर्ड, और स्वास्थ्य संबंधी जानकारी।
4. **कॉर्पोरेट डेटा (Corporate Data):**
   * व्यापार योजनाएँ, बौद्धिक संपदा, और संविदा दस्तावेज।

SCERT DELHI

डेटा की सुरक्षा के उपाय

1. डेटा एन्क्रिप्शन (Data Encryption):

* संवेदनशील डेटा को एन्क्रिप्ट किया जाता है ताकि अनधिकृत व्यक्ति इसे न पढ़ सकें।

2. एक्सेस नियंत्रण (Access Control):

* यह सुनिश्चित करता है कि केवल अधिकृत उपयोगकर्ता ही डेटा तक पहुँच सकें।

3. डेटा बैकअप (Data Backup):

* नियमित रूप से डेटा का बैकअप लिया जाता है ताकि डेटा खोने की स्थिति में उसे पुनर्स्थापित किया जा सके।

4. फायरवॉल और सुरक्षा सॉफ़्टवेयर (Firewall and Security Software):

* नेटवर्क और सिस्टम की सुरक्षा के लिए फायरवॉल और एंटीवायरस सॉफ्टवेयर का उपयोग किया जाता है।

5. सुरक्षा नीतियाँ (Security Policies):

* संगठनों में डेटा सुरक्षा से संबंधित नियम और प्रक्रियाएँ लागू की जाती हैं।

सुरक्षित डेटा का आरेख (Diagram)

```
                     सुरक्षित डेटा (Protected Data)
                                  |
        -----------------------------------------------------
        |                         |                         |
 व्यक्तिगत डेटा          वित्तीय डेटा                   स्वास्थ्य डेटा
        |                         |                         |
नाम, पता, ईमेल         बैंक विवरण, क्रेडिट कार्ड        चिकित्सा रिकॉर्ड
                                  |
                           कॉर्पोरेट डेटा
                                  |
                      व्यापार योजनाएँ, संविदाएँ
                                  |
                     ----------------------------
                     |                          |
              डेटा एन्क्रिप्शन              एक्सेस नियंत्रण
                     |                          |
```

4.6 फायरवॉल के उपयोग

फायरवॉल एक सुरक्षा उपकरण है जो नेटवर्क की सुरक्षा सुनिश्चित करने में महत्वपूर्ण भूमिका निभाता है। यह अवांछित नेटवर्क ट्रैफ़िक को रोकता है और सुरक्षा नीतियों के आधार पर डेटा पैकेट्स को नियंत्रित करता है। फायरवॉल का उपयोग किसी संगठन या व्यक्तिगत उपयोगकर्ता के सिस्टम को बाहरी खतरों से बचाने के लिए किया जाता है।

फायरवॉल के उपयोग के लाभ

1. **नेटवर्क सुरक्षा (Network Security):**
   * फायरवॉल नेटवर्क पर आने-जाने वाले ट्रैफिक की निगरानी करता है और अवांछित या संदिग्ध गतिविधियों को रोकता है।
2. **डेटा की सुरक्षा (Data Protection):**
   * संवेदनशील डेटा को सुरक्षित रखने के लिए यह अवांछित एक्सेस को रोकता है।
3. **हमलों की पहचान (Intrusion Detection):**
   * यह संदिग्ध गतिविधियों की पहचान करने में मदद करता है, जिससे साइबर हमलों का पता लगाया जा सकता है।
4. **सुरक्षा नीतियों का पालन (Enforcement of Security Policies):**
   * संगठन की सुरक्षा नीतियों को लागू करने में मदद करता है, जैसे कि कौन सी सेवाएँ या प्रोटोकॉल उपयोग किए जा सकते हैं।
5. **रिपोर्टिंग और लॉगिंग (Reporting and Logging):**
   * फायरवॉल नेटवर्क गतिविधियों को लॉगिंग करता है, जिससे नेटवर्क पर होने वाली घटनाओं का पता लगाने में मदद मिलती है।

फायरवॉल के प्रकार

1. **नेटवर्क फायरवॉल (Network Firewall):**
   * यह एक हार्डवेयर या सॉफ्टवेयर समाधान हो सकता है जो नेटवर्क ट्रैफिक को नियंत्रित करता है।

SCERT DELHI

2. हॉस्ट-आधारित फायरवॉल (Host-based Firewall):

* यह व्यक्तिगत कंप्यूटर पर स्थापित किया जाता है और स्थानीय स्तर पर सुरक्षा प्रदान करता है।

3. स्टेटफुल फायरवॉल (Stateful Firewall):

* यह ट्रैफिक के स्टेट को ट्रैक करता है और सुरक्षा नियमों के अनुसार निर्णय लेता है।

4. पैकेट फिल्टरिंग फायरवॉल (Packet Filtering Firewall):

* यह नेटवर्क पैकेट्स के हेडर की जानकारी के आधार पर अनुमति या ब्लॉक करता है।

फायरवॉल का आरेख (Diagram)

```
                    सुरक्षित डेटा (Protected Data)
                                |
        --------------------------------------------------
        |                       |                        |
   व्यक्तिगत डेटा          वित्तीय डेटा                 स्वास्थ्य डेटा
        |                       |                        |
 नाम, पता, ईमेल        बैंक विवरण, क्रेडिट कार्ड        चिकित्सा रिकॉर्ड
                                |
                          कॉर्पोरेट डेटा
                                |
                  व्यापार योजनाएँ, संविदाएँ
                                |
                    --------------------------
                    |                        |
           डेटा एन्क्रिप्शन               एक्सेस नियंत्रण
                    |                        |
        संवेदनशील डेटा की सुरक्षा     अधिकृत उपयोगकर्ता पहुँच
```

4.7 एप्लिकेशन लेवल गेटवे प्रॉक्सी फायरवॉल

एप्लिकेशन लेवल गेटवे प्रॉक्सी फायरवॉल एक प्रकार का फायरवॉल है जो नेटवर्क ट्रैफिक को एप्लिकेशन स्तर पर नियंत्रित करता है। यह फायरवॉल विशेष रूप से उपयोगकर्ताओं और एप्लिकेशन के बीच एक मध्यस्थ के रूप में कार्य करता है। यह सुरक्षा सुनिश्चित करने के लिए एप्लिकेशन डेटा की गहराई से निगरानी करता है।

एप्लिकेशन लेवल गेटवे प्रॉक्सी फायरवॉल की विशेषताएँ

1. मध्यस्थता (Proxying):

* यह उपयोगकर्ताओं के अनुरोधों को रिसीव करता है और फिर उन्हें लक्ष्य सर्वर पर भेजता है, जिससे उपयोगकर्ताओं की पहचान छिपी रहती है।

2. डेटा फिल्टरिंग (Data Filtering):

* फायरवॉल एप्लिकेशन डेटा की गहराई से जांच करता है और यह सुनिश्चित करता है कि केवल अनुमत डेटा ही नेटवर्क में प्रवेश कर सके।

3. सुरक्षा नीतियाँ (Security Policies):

* यह सुरक्षा नीतियों को लागू करता है, जैसे कि कौन से एप्लिकेशन या सेवाएँ अनुमति प्राप्त हैं।

4. हमले की पहचान (Intrusion Detection):

* संदिग्ध गतिविधियों का पता लगाने और हमलों को रोकने के लिए यह सिस्टम गतिविधियों की निगरानी करता है।

5. अनुमति और अस्वीकृति (Allow and Deny):

* यह निर्णय लेता है कि कौन से अनुरोधों को अनुमति दी जाए और कौन से अस्वीकृत किए जाएं।

एप्लिकेशन लेवल गेटवे प्रॉक्सी फायरवॉल के लाभ

1. उच्च सुरक्षा (High Security):

* एप्लिकेशन लेवल पर गहराई से स्कैनिंग के कारण यह अधिक सुरक्षा प्रदान करता है।

2. उपयोगकर्ता की पहचान की सुरक्षा (User Identity Protection):

* उपयोगकर्ता की पहचान को छिपा कर रखने की क्षमता इसे विशेष बनाती है।

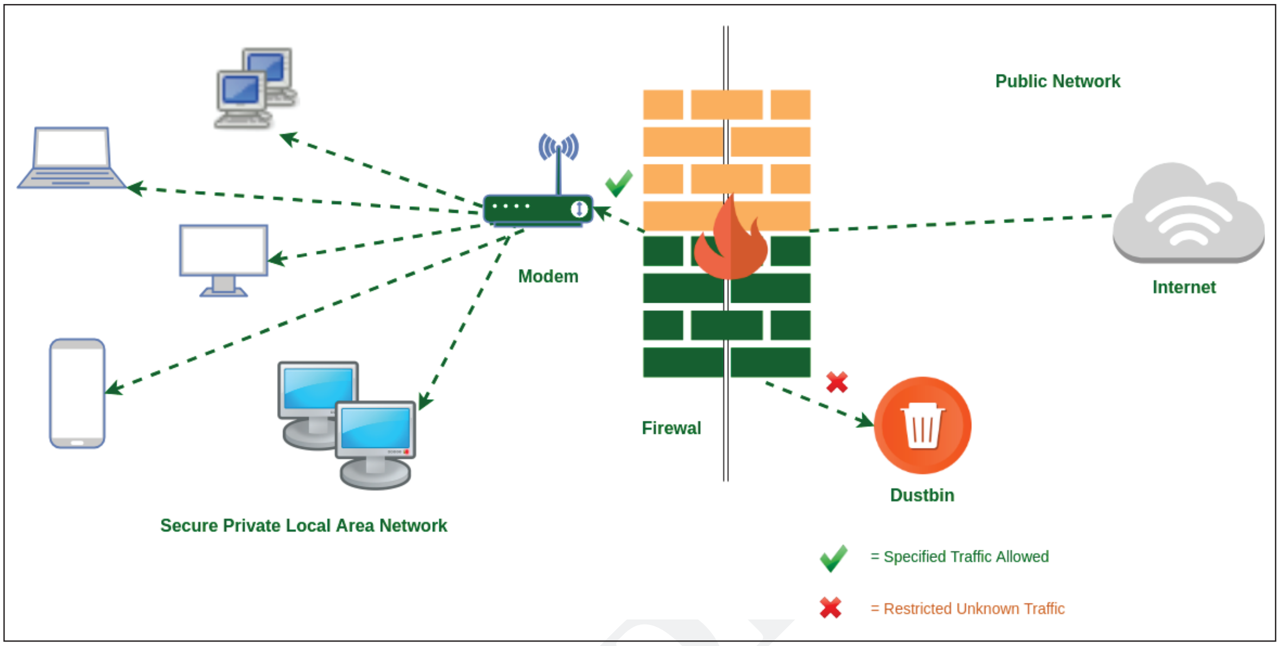
3. कम नेटवर्क ट्रैफिक (Reduced Network Traffic):

* प्रॉक्सी फायरवॉल केवल अनुमत ट्रैफिक को आगे बढ़ाता है, जिससे नेटवर्क पर अनावश्यक लोड कम होता है।

SCERT DELHI

4. उन्नत रिपोर्टिंग (Advanced Reporting):

* यह सुरक्षा की स्थिति के बारे में विस्तृत रिपोर्ट प्रदान करता है।



अपनी प्रगति जाँचें

अ. बहु विकल्पीय प्रश्न

1. आईटी सुरक्षा का मुख्य उद्देश्य क्या है?

A. केवल डेटा का बैकअप लेना

B. डेटा और सिस्टम को unauthorized एक्सेस से सुरक्षित रखना

C. केवल सॉफ्टवेयर अपडेट करना

D. नेटवर्क का विस्तार करना

2. एंटीवायरस सॉफ्टवेयर का प्रमुख कार्य क्या है?

A. केवल ईमेल भेजना

B. वायरस और अन्य दुर्भावनापूर्ण सॉफ्टवेयर को पहचानना और हटाना

C. सिस्टम की गति बढ़ाना

D. फ़ाइलों को संकुचित करना

3. कमजोरियों (vulnerabilities) का क्या अर्थ है?

A. कंप्यूटर में डेटा का होना
B. सुरक्षा के लिए कमजोर बिंदु
C. सॉफ्टवेयर अपडेट की आवश्यकता
D. सिस्टम का धीमा होना

4. सुरक्षा प्रक्रियाएँ (Security Procedures) का क्या महत्व है?

A. डेटा को अनधिकृत एक्सेस से बचाना
B. सॉफ्टवेयर की गुणवत्ता बढ़ाना
C. केवल हार्डवेयर को सुरक्षित रखना
D. नेटवर्क को सुचारु रूप से चलाना

5. सुरक्षित डेटा (Protected Data) का मुख्य लक्ष्य क्या है?

A. डेटा का बैकअप लेना
B. डेटा की गोपनीयता और सुरक्षा सुनिश्चित करना
C. डेटा को साझा करना
D. डेटा को डिलीट करना

6. फायरवॉल का मुख्य कार्य क्या है?

A. केवल डेटा स्टोर करना
B. नेटवर्क ट्रैफिक को नियंत्रित करना और सुरक्षा प्रदान करना
C. सॉफ्टवेयर इंस्टॉल करना
D. केवल नेटवर्क की गति बढ़ाना

7. एप्लिकेशन लेवल गेटवे प्रॉक्सी फायरवॉल क्या करता है?

A. केवल डेटा को संकुचित करता है
B. एप्लिकेशन स्तर पर ट्रैफिक को नियंत्रित करता है
C. फाइलों को भेजता है
D. नेटवर्क की गति बढ़ाता है

SCERT DELHI

8. आईटी सुरक्षा में कौन सा उपाय डेटा सुरक्षा के लिए सबसे महत्वपूर्ण है?

A. नियमित सॉफ्टवेयर अपडेट
B. केवल पासवर्ड का उपयोग
C. नेटवर्क का विस्तार
D. हार्डवेयर को अपग्रेड करना

9. सुरक्षा प्रक्रियाओं का पालन क्यों किया जाना चाहिए?

A. केवल कॉर्पोरेट नीतियों के लिए
B. डेटा और सिस्टम की सुरक्षा सुनिश्चित करने के लिए
C. केवल कर्मचारियों की निगरानी के लिए
D. नेटवर्क की गति बढ़ाने के लिए

10. एंटीवायरस सॉफ्टवेयर को नियमित रूप से अपडेट करना क्यों आवश्यक है?

A. सिस्टम की गति बढ़ाने के लिए
B. नए वायरस और हमलों के खिलाफ सुरक्षा सुनिश्चित करने के लिए
C. केवल पुराने डेटा को हटाने के लिए
D. हार्डवेयर को अपग्रेड करने के लिए

ब. लघु उत्तरीय प्रश्न

1. आईटी सुरक्षा का मुख्य सिद्धांत क्या है?
2. एंटीवायरस सॉफ्टवेयर का उपयोग क्यों आवश्यक है?
3. कमज़ोरियाँ (vulnerabilities) का क्या अर्थ है?
4. सुरक्षा प्रक्रियाएँ (Security Procedures) क्यों महत्वपूर्ण हैं?
5. फायरवॉल का क्या कार्य है?

SCERT DELHI

आईटीआईएल v3 की मूल बातें

अध्याय 5

परिचय

आईटीआईएल (Information Technology Infrastructure Library) एक सर्वश्रेष्ठ प्रथा (Best Practice) ढांचा है, जिसका उपयोग आईटी सेवा प्रबंधन (IT Service Management) के लिए किया जाता है। यह ढांचा संगठनों को आईटी सेवाओं को प्रभावी ढंग से प्रबंधित करने, ग्राहक संतोष को बढ़ाने और व्यावसायिक उद्देश्यों को प्राप्त करने में मदद करता है। आईटीआईएल का उद्देश्य आईटी सेवाओं को उनके संपूर्ण जीवन चक्र के दौरान प्रबंधित करना है।

आईटीआईएल v3 का परिचय

आईटीआईएल का तीसरा संस्करण (v3) 2007 में जारी किया गया था और इसमें पहले के संस्करणों की तुलना में कई महत्वपूर्ण सुधार और अद्यतन शामिल किए गए हैं। आईटीआईएल v3 में सेवाओं के जीवन चक्र को समझने के लिए एक संरचना प्रदान की गई है।

5.1 आईटीआईएल की आवश्यकता (Requirement of ITIL)

आईटीआईएल (Information Technology Infrastructure Library) एक सर्वश्रेष्ठ प्रथा ढांचा है जो आईटी सेवा प्रबंधन (IT Service Management) के लिए विकसित किया गया है।

आज की डिजिटल दुनिया में, जहां प्रौद्योगिकी व्यवसाय संचालन का एक महत्वपूर्ण हिस्सा बन चुकी है, आईटीआईएल के उपयोग की आवश्यकता और भी अधिक बढ़ गई है।

आईटीआईएल की आवश्यकता के प्रमुख कारण

1. **सर्विस की गुणवत्ता में सुधार (Improvement in Service Quality):**
   * आईटीआईएल प्रक्रियाएँ सेवाओं की गुणवत्ता में सुधार करती हैं, जिससे उपयोगकर्ताओं को बेहतर अनुभव मिलता है।
2. **उपयोगकर्ता संतोष (User Satisfaction):**
   * सेवाओं को बेहतर ढंग से प्रबंधित करने से उपयोगकर्ताओं का संतोष बढ़ता है, जो व्यवसाय की सफलता के लिए महत्वपूर्ण है।
3. **प्रदर्शन में सुधार (Performance Improvement):**
   * आईटीआईएल के अंतर्गत प्रक्रियाएँ संगठन की दक्षता और प्रदर्शन में सुधार करती हैं।
4. **खर्चों में कमी (Cost Reduction):**
   * आईटीआईएल का उपयोग करके संगठन संसाधनों का बेहतर प्रबंधन कर सकते हैं, जिससे लागत में कमी आती है।
5. **रिस्क प्रबंधन (Risk Management):**
   * आईटीआईएल प्रक्रियाएँ जोखिमों की पहचान और प्रबंधन में मदद करती हैं, जिससे सुरक्षा बढ़ती है।
6. **संवेदनशीलता और लचीलापन (Sensitivity and Flexibility):**
   * आईटीआईएल संगठनों को बदलती परिस्थितियों के अनुसार अपनी सेवाओं को समायोजित करने की क्षमता प्रदान करता है।

SCERT DELHI

आईटीआईएल की आवश्यकता का आरेख (Diagram)

```
                    आईटीआईएल की आवश्यकता
                    (Requirement of ITIL)
                              |
         ---------------------------------------------------
         |               |                |                |
  सेवा गुणवत्ता     उपयोगकर्ता संतोष   प्रदर्शन में सुधार   खर्चों में कमी
         |               |                |                |
  उच्च गुणवत्ता        ग्राहक अनुभव       बेहतर दक्षता       बेहतर संसाधन प्रबंधन
         |
  -----------------------------------
  |              |                |
रिस्क प्रबंधन    संवेदनशीलता          लचीलापन
```

5.2 आईटीआईएल के संस्करण (versions of ITIL)

आईटीआईएल (Information Technology Infrastructure Library) विभिन्न संस्करणों में विकसित हुआ है। प्रत्येक संस्करण में आईटी सेवा प्रबंधन (IT Service Management) के लिए नई विधियाँ, तकनीकें और प्रक्रियाएँ शामिल की गई हैं। आईटीआईएल का लक्ष्य संगठन की आईटी सेवाओं को बेहतर ढंग से प्रबंधित करना है।

आईटीआईएल के प्रमुख संस्करण

1. आईटीआईएल v1 (ITIL v1):

* **जारी किया गया:** 1980 के दशक में
* **विशेषता:** पहला आधिकारिक आईटीआईएल संस्करण, जो आईटी सेवा प्रबंधन पर केंद्रित था। इसमें मूलभूत प्रक्रियाएँ और प्राथमिकताएँ शामिल थीं।

2. आईटीआईएल v2 (ITIL v2):

* **जारी किया गया:** 2000 में
* **विशेषता:** इसमें विभिन्न आईटी प्रबंधन प्रक्रियाओं को अधिक स्पष्टता के साथ परिभाषित किया गया। इसे "सेवा प्रबंधन" के चार प्रमुख क्षेत्रों में विभाजित किया गया।

3. आईटीआईएल v3 (ITIL v3):

* **जारी किया गया:** 2007 में

SCERT DELHI

* **विशेषताः** इसमें सेवा जीवन चक्र (Service Lifecycle) पर ध्यान केंद्रित किया गया। इसे पाँच चरणों में विभाजित किया गया सेवा रणनीति, सेवा डिज़ाइन, सेवा संक्रमण, सेवा संचालन, और सतत सेवा सुधार।

4. आईटीआईएल 2011 (ITIL 2011):

* **जारी किया गयाः** 2011 में
* **विशेषताः** यह आईटीआईएल v3 का अद्यतन संस्करण है। इसमें कुछ प्रक्रियाओं और परिभाषाओं में सुधार किया गया और कुछ महत्वपूर्ण मुद्दों को संबोधित किया गया।

5. आईटीआईएल 4 (ITIL 4):

* **जारी किया गयाः** 2019 में
* **विशेषताः** आईटीआईएल 4 ने सेवा प्रबंधन के साथ-साथ डिजिटल परिवर्तन (Digital Transformation) और अन्य आधुनिक प्रवृत्तियों पर ध्यान केंद्रित किया। यह Agile, DevOps, और Lean प्रथाओं के साथ समेकित हुआ।

आईटीआईएल के संस्करणों का आरेख (Diagram)

```
                  आईटीआईएल (ITIL)
                         |
      -----------------------------------
      |                  |                 |
   ITIL v1           ITIL v2           ITIL v3
   (1980)             (2000)            (2007)
                         |
              ----------------
              |               |
          ITIL 2011       ITIL 4
            (2011)        (2019)
```

5.3 आईटीआईएल प्रकाशन (ITIL Publications)

आईटीआईएल (Information Technology Infrastructure Library) विभिन्न प्रकाशनों के माध्यम से आईटी सेवा प्रबंधन (IT Service Management) के लिए सर्वोत्तम प्रथाओं और मार्गदर्शिकाएँ प्रदान करता है। ये प्रकाशन संगठनों को अपनी आईटी सेवाओं को बेहतर ढंग से प्रबंधित करने और कार्यक्षमता बढ़ाने में मदद करते हैं।

आईटीआईएल के प्रमुख प्रकाशन

1. आईटीआईएल फाउंडेशन (ITIL Foundation):

* यह प्रकाशन आईटीआईएल के मूल सिद्धांतों और अवधारणाओं का परिचय देता है। यह आईटी सेवा प्रबंधन के क्षेत्र में शुरुआत करने वालों के लिए उपयुक्त है।

2. सेवा रणनीति (Service Strategy):

* यह प्रकाशन सेवा रणनीति की योजना बनाने, विकास करने और प्रबंधन करने के लिए दिशानिर्देश प्रदान करता है। इसमें सेवा प्रबंधन के व्यावसायिक दृष्टिकोण को समझाया गया है।

3. सेवा डिज़ाइन (Service Design):

* यह प्रकाशन नई सेवाओं के डिजाइन, योजना और सुधार के लिए प्रक्रियाओं और तकनीकों पर ध्यान केंद्रित करता है।

4. सेवा संक्रमण (Service Transition):

* यह प्रकाशन नई या परिवर्तित सेवाओं को प्रभावी ढंग से उत्पादन में लाने के लिए आवश्यक प्रक्रियाएँ और उपकरण प्रदान करता है।

5. सेवा संचालन (Service Operation):

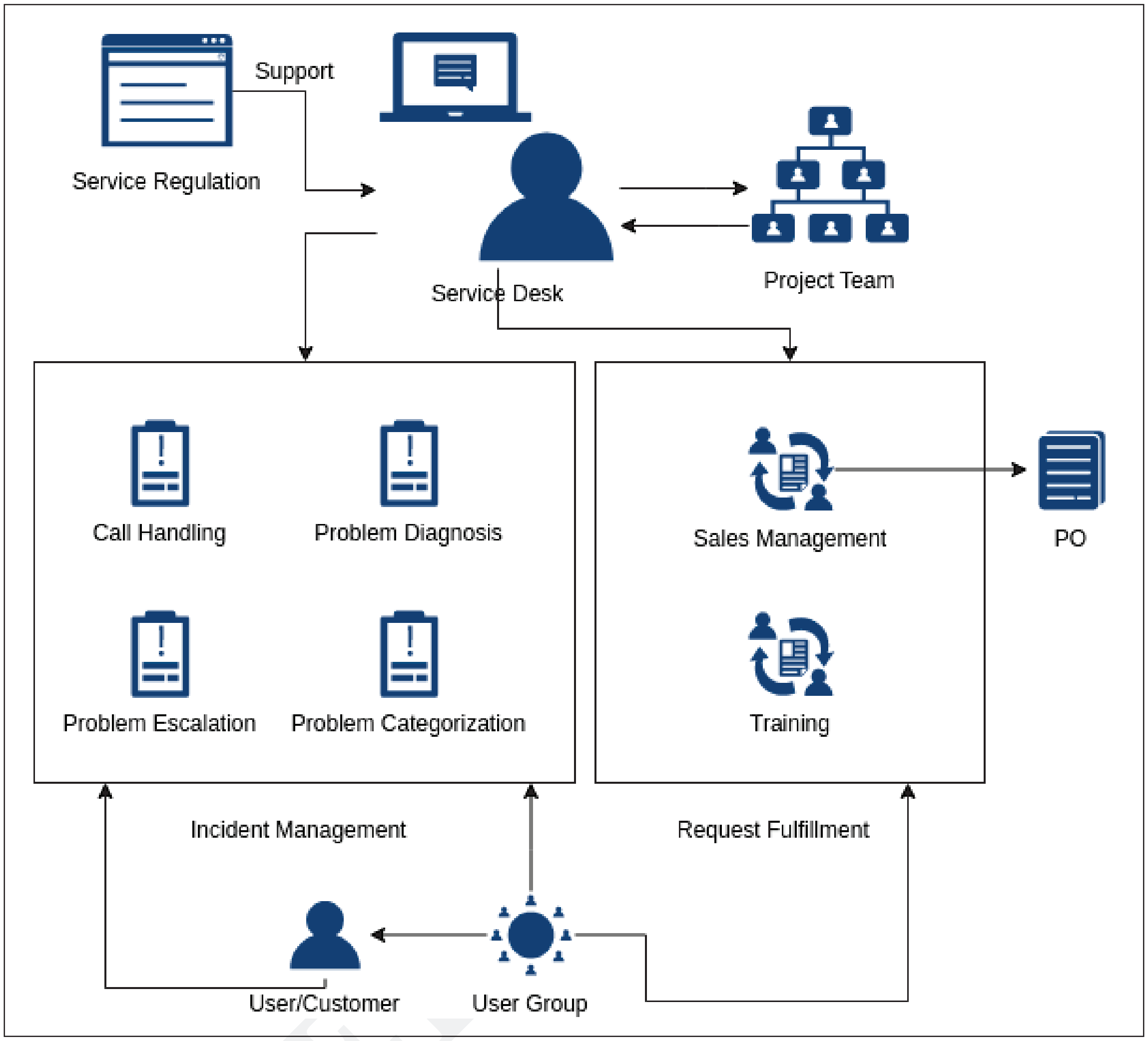
* यह प्रकाशन सेवा संचालन में सर्वोत्तम प्रथाओं को बताता है, जिसमें सेवा अनुरोध, घटना प्रबंधन और समस्या प्रबंधन शामिल हैं।

6. सतत सेवा सुधार (Continual Service Improvement):

* यह प्रकाशन आईटी सेवाओं के निरंतर सुधार की प्रक्रिया के लिए दिशानिर्देश प्रदान करता है। इसमें सुधार के लिए मापदंड और तकनीकें शामिल हैं।

SCERT DELHI

आईटीआईएल प्रकाशनों का आरेख (Diagram)



5.4 आईटीआईएल के लाभ (Benefits of ITIL)

आईटीआईएल (Information Technology Infrastructure Library) एक उत्कृष्ट ढांचा है जो आईटी सेवा प्रबंधन (IT Service Management) के लिए सर्वोत्तम प्रथाओं और तकनीकों को परिभाषित करता है। इसके उपयोग के कई लाभ हैं, जो संगठनों को उनकी आईटी सेवाओं को बेहतर ढंग से प्रबंधित करने में मदद करते हैं। नीचे आईटीआईएल के कुछ प्रमुख लाभ दिए गए हैं:

1. सेवा की गुणवत्ता में सुधार (Improvement in Service Quality):

आईटीआईएल के उपयोग से संगठनों को उच्च गुणवत्ता वाली सेवाएँ प्रदान करने में मदद मिलती है। मानकीकृत प्रक्रियाएँ और तकनीकें सेवाओं की विश्वसनीयता और स्थिरता को बढ़ाती हैं।

2. **उपयोगकर्ता संतोष (User Satisfaction):**

आईटीआईएल के सिद्धांतों का पालन करने से ग्राहक की आवश्यकताओं को बेहतर ढंग से समझा जा सकता है, जिससे उपयोगकर्ता संतोष में वृद्धि होती है। जब सेवाएँ कुशलता से प्रदान की जाती हैं, तो ग्राहक अधिक संतुष्ट होते हैं।

3. **लागत में कमी (Cost Reduction):**

आईटीआईएल प्रक्रियाओं के कार्यान्वयन से संगठन संसाधनों का बेहतर उपयोग कर सकते हैं, जिससे कुल संचालन लागत में कमी आती है। प्रक्रियाओं को मानकीकृत करने से समय और प्रयास की बचत होती है।

4. **प्रदर्शन में सुधार (Performance Improvement):**

आईटीआईएल के उपयोग से संगठन की कार्यक्षमता और प्रदर्शन में सुधार होता है। स्पष्ट प्रक्रियाएँ और मापदंडों की स्थापना से प्रदर्शन का मूल्यांकन करना आसान होता है।

5. **जोखिम प्रबंधन (Risk Management):**

आईटीआईएल संगठनों को संभावित जोखिमों की पहचान और प्रबंधन के लिए आवश्यक दिशा-निर्देश प्रदान करता है। इससे सुरक्षा में वृद्धि होती है और संगठन अधिक सुरक्षित बनते हैं।

6. **निरंतर सुधार (Continual Improvement):**

आईटीआईएल संगठनों को निरंतर सुधार के लिए प्रेरित करता है। इसमें सेवाओं के निरंतर मूल्यांकन और सुधार की प्रक्रिया शामिल है, जिससे सेवाएँ समय के साथ विकसित होती रहती हैं।

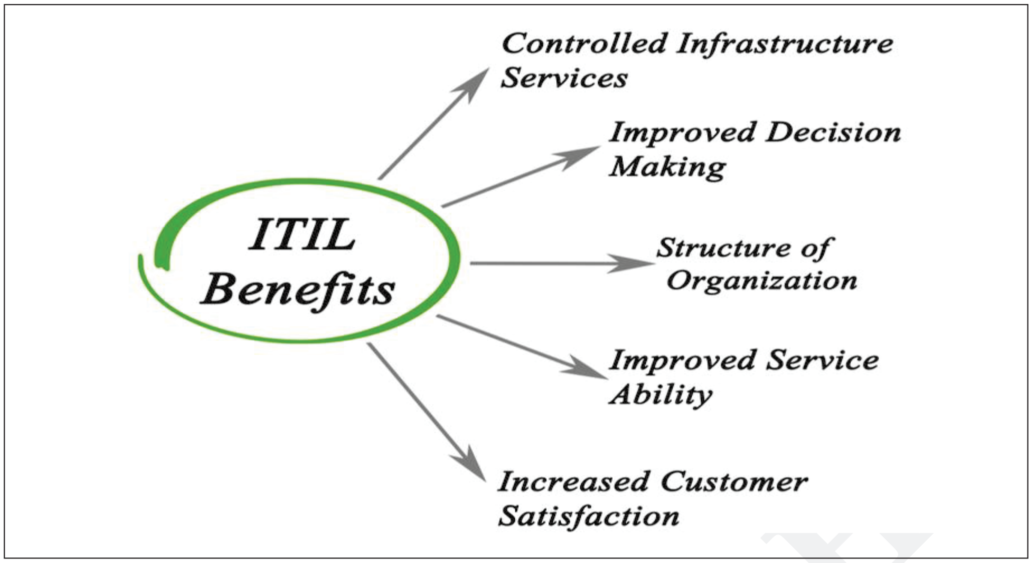
7. **निर्णय लेने में सहायता (Assistance in Decision Making):**

आईटीआईएल के अंतर्गत प्रक्रियाएँ और डेटा संगठनों को सही निर्णय लेने में सहायता करते हैं। संगठनों के पास उचित जानकारी होती है, जिससे वे बेहतर रणनीतियाँ विकसित कर सकते हैं।

8. **प्रशिक्षण और विकास (Training and Development):**

आईटीआईएल संगठनों के कर्मचारियों को आईटी सेवा प्रबंधन के क्षेत्र में प्रशिक्षित करने में मदद करता है। यह उनके कौशल और ज्ञान को बढ़ाने का अवसर प्रदान करता है।

SCERT DELHI



5.5 आईटीआईएल v2 बनाम आईटीआईएल v3 (ITIL v2 vs ITIL v3)

आईटीआईएल (Information Technology Infrastructure Library) समय के साथ विकसित हुआ है, और इसके विभिन्न संस्करणों ने आईटी सेवा प्रबंधन (IT Service Management) में महत्वपूर्ण बदलाव किए हैं। आईटीआईएल v2 और v3 के बीच के प्रमुख अंतरों को निम्नलिखित बिंदुओं के माध्यम से समझाया गया है:

1. संरचना (Structure)

आईटीआईएल v2: आईटीआईएल v2 में 8 पुस्तकें शामिल थीं, जो मुख्यतः आईटी सेवा प्रबंधन के विभिन्न पहलुओं पर केंद्रित थीं। इसे चार प्रमुख क्षेत्रों में विभाजित किया गया था: सेवा समर्थन (Service Support), सेवा प्रबंधन (Service Delivery), और ITIL के अन्य घटक।

आईटीआईएल v3: आईटीआईएल v3 में सेवा जीवन चक्र (Service Lifecycle) की अवधारणा पर जोर दिया गया है। इसे पाँच प्रमुख चरणों में विभाजित किया गया है:

1. सेवा रणनीति (Service Strategy)
2. सेवा डिज़ाइन (Service Design)
3. सेवा संक्रमण (Service Transition)

SCERT DELHI

4. सेवा संचालन (Service Operation)

5. सतत सेवा सुधार (Continual Service Improvement)

2. ध्यान केंद्रित क्षेत्र (Focus Areas)

आईटीआईएल v2: मुख्य रूप से आईटी सेवा प्रबंधन प्रक्रियाओं पर ध्यान केंद्रित किया गया, जिसमें अधिकतर प्रक्रियाओं और कार्यों को परिभाषित किया गया था।

आईटीआईएल v3: आईटीआईएल v3 ने सेवा जीवन चक्र की पूरी प्रक्रिया को समझने पर ध्यान केंद्रित किया है, जिससे संगठन अपने आईटी सेवाओं की योजना, डिजाइन, कार्यान्वयन, और सुधार कर सकें।

3. प्रक्रिया और कार्यान्वयन (Processes and Implementation)

आईटीआईएल v2: प्रक्रियाओं की स्पष्टता और कार्यान्वयन में कुछ सीमाएँ थीं, जिससे कुछ संगठनों के लिए इसे अपनाना मुश्किल हो सकता था।

आईटीआईएल v3: आईटीआईएल v3 ने प्रक्रियाओं को और अधिक स्पष्टता और व्यावहारिकता के साथ प्रस्तुत किया है। इसमें प्रक्रियाओं को समेकित रूप से देखने और उन्हें एक दूसरे से संबंधित करने की क्षमता है।

4. उपयोगकर्ताओं की आवश्यकताएँ (User Needs)

आईटीआईएल v2: उपयोगकर्ताओं की आवश्यकताओं पर अधिक ध्यान नहीं दिया गया था। यह मुख्य रूप से प्रक्रियाओं और कार्यों पर केंद्रित था।

आईटीआईएल v3: उपयोगकर्ताओं की आवश्यकताओं और अनुभवों को प्राथमिकता दी गई है। यह ग्राहकों के लिए उच्च गुणवत्ता वाली सेवाएँ प्रदान करने पर केंद्रित है।

5. प्रशिक्षण और प्रमाणन (Training and Certification)

आईटीआईएल v2: आईटीआईएल v2 के लिए प्रशिक्षण और प्रमाणन सीमित थे।

आईटीआईएल v3: आईटीआईएल v3 ने अधिक संरचित और मानकीकृत प्रशिक्षण और प्रमाणन कार्यक्रमों की पेशकश की है, जिससे कर्मचारियों को बेहतर तरीके से प्रशिक्षित किया जा सकता है।

SCERT DELHI

5.6 सेवा (Service) की अवधारणाएँ

सेवा (Service) एक ऐसी गतिविधि या कार्य है जो किसी अन्य व्यक्ति या संगठन के लाभ के लिए किया जाता है। आईटी सेवा प्रबंधन (IT Service Management) में, ग्राहकों की आवश्यकताओं को पूरा करने के लिए सेवाओं का निर्माण और प्रबंधन किया जाता है। सेवाएँ मुख्यतः दो प्रकार की होती हैं: आंतरिक ग्राहक (Internal Customer) और बाहरी ग्राहक (External Customer)। इन दोनों की अवधारणाएँ निम्नलिखित हैं:

a. आंतरिक ग्राहक (Internal Customer)

आंतरिक ग्राहक वह व्यक्ति या समूह होता है जो किसी संगठन के भीतर कार्य करता है और जिसकी आवश्यकताओं को पूरा करने के लिए सेवाएँ प्रदान की जाती हैं। ये ग्राहक संगठन के विभिन्न विभागों या टीमों से संबंधित हो सकते हैं।

विशेषताएँ:

1. **संबंध:** आंतरिक ग्राहक आमतौर पर संगठन के कर्मचारियों या टीमों का हिस्सा होते हैं। उनके साथ काम करना अक्सर सहकारी और सामूहिक होता है।
2. **उदाहरण** - एक आईटी टीम का सदस्य जो सिस्टम समर्थन सेवा का उपयोग कर रहा है या मानव संसाधन विभाग का कर्मचारी जो वेतन की जानकारी प्राप्त कर रहा है।
3. **महत्वः** आंतरिक ग्राहकों की संतोषजनक सेवाएँ संगठन के भीतर कार्यक्षमता और उत्पादनशीलता को बढ़ाती हैं।

b. बाहरी ग्राहक (External Customer)

बाहरी ग्राहक वह व्यक्ति या संगठन होता है जो किसी सेवा या उत्पाद का उपयोग करता है, लेकिन वह उस संगठन का हिस्सा नहीं होता। बाहरी ग्राहक संगठन के द्वारा प्रदान की गई सेवाओं के लिए भुगतान कर सकते हैं और उनके अनुभव का संगठन की छवि पर बड़ा प्रभाव होता है।

5.7 आईटी सेवा प्रबंधन (IT Service Management)

आईटी सेवा प्रबंधन (IT Service Management या ITSM) एक ऐसी प्रक्रिया है जिसका उद्देश्य आईटी सेवाओं के प्रभावी और कुशल प्रबंधन के माध्यम से व्यवसाय की आवश्यकताओं को पूरा करना है। यह प्रक्रियाओं, तकनीकों और सर्वोत्तम प्रथाओं का एक समूह है, जिसका लक्ष्य आईटी सेवाओं की

SCERT DELHI

गुणवत्ता, दक्षता और प्रभावशीलता को बढ़ाना है।

5.7.1 आईटी सेवा प्रबंधन (ITSM) का महत्व

आईटी सेवा प्रबंधन (ITSM) का महत्व निम्नलिखित बिंदुओं में देखा जा सकता है:

1. **व्यापारिक संरेखण:** आईटी सेवाएँ व्यापारिक लक्ष्यों के साथ संरेखित होती हैं, जिससे निर्णय लेने में मदद मिलती है।
2. **सेवा की गुणवत्ता:** मानकीकृत प्रक्रियाएँ सेवा की गुणवत्ता और विश्वसनीयता को बढ़ाती हैं।
3. **ग्राहक संतोष:** बेहतर सेवाएँ ग्राहक संतोष को बढ़ाती हैं, जिससे ग्राहकों को बनाए रखने में मदद मिलती है।
4. **लागत में कमी:** संसाधनों का अनुकूलन और प्रक्रियाओं की कुशलता से परिचालन लागत कम होती है।
5. **जोखिम प्रबंधन:** संभावित जोखिमों की पहचान और प्रबंधन से सेवा में व्यवधानों को कम किया जा सकता है।
6. **निरंतर सुधार:** नियमित मूल्यांकन के माध्यम से सेवाओं में निरंतर सुधार संभव है।

5.7.2 सेवा में हितधारक

सेवा में हितधारक वे व्यक्ति या समूह होते हैं जो किसी सेवा से प्रभावित होते हैं या जिनका सेवा पर प्रभाव होता है। प्रमुख हितधारकों में शामिल हैं:

1. **ग्राहक (Customers):** सेवा का उपयोग करने वाले लोग, जिनकी संतोषजनक अनुभव महत्वपूर्ण है।

SCERT DELHI

2. **सेवा प्रदाता (Service Providers):** वे संगठन या व्यक्ति जो सेवाएँ प्रदान करते हैं।

3. **प्रबंधक (Managers):** सेवाओं का संचालन और रणनीतिक निर्णय लेने वाले व्यक्ति।

4. **कर्मचारी (Employees):** सेवा प्रदाता के लिए काम करने वाले लोग, जिनकी दक्षता सेवाओं की गुणवत्ता को प्रभावित करती है।

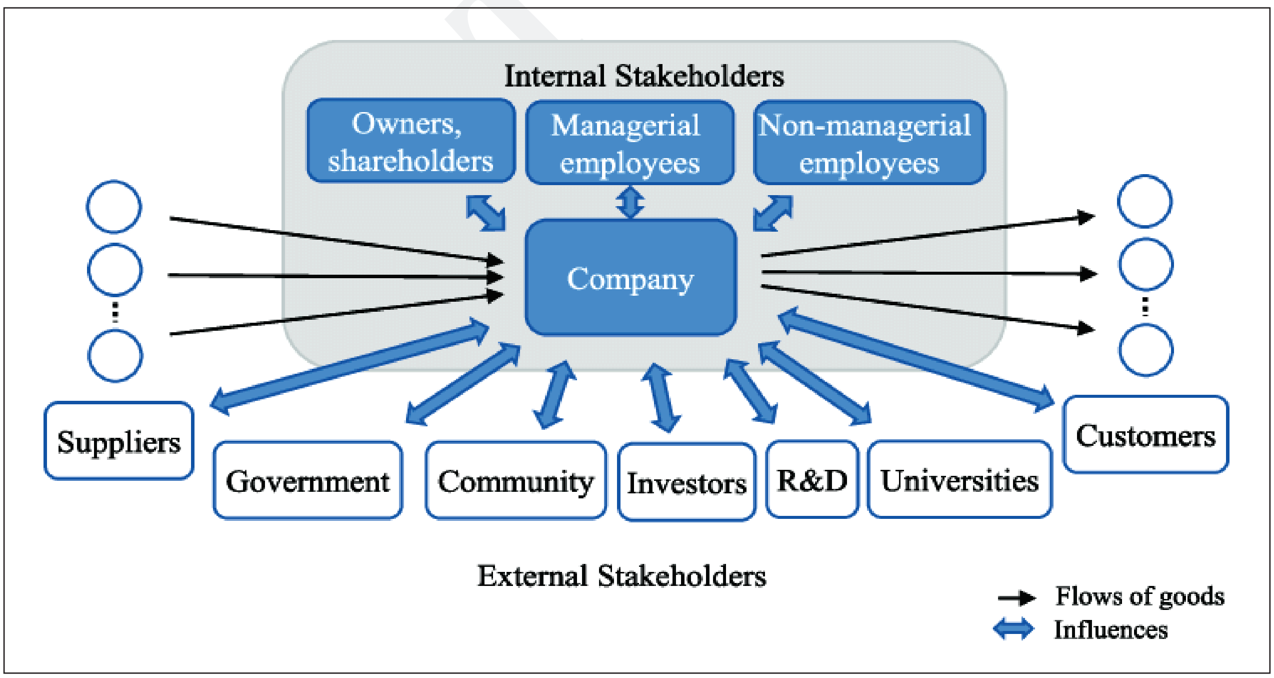
5. **आपूर्तिकर्ता (Suppliers):** आवश्यक संसाधन और सामग्री प्रदान करने वाले व्यक्ति या कंपनियाँ।

6. **साझेदार (Partners):** वे संगठन जो सेवा प्रदाता के साथ सहयोग करते हैं।

7. **नियामक संस्थाएँ (Regulatory Bodies):** मानक और नियम निर्धारित करने वाली संस्थाएँ।

8. **समुदाय (Community):** स्थानीय समुदाय, जिनकी आवश्यकताओं को ध्यान में रखना सामाजिक जिम्मेदारी का हिस्सा है।

इन हितधारकों की पहचान और उनकी आवश्यकताओं को समझना सेवा प्रबंधन की सफलता के लिए आवश्यक है।



5.8 समस्या प्रबंधन (Problem Management)

समस्या प्रबंधन (Problem Management) आईटी सेवा प्रबंधन (IT Service Management) का एक महत्वपूर्ण हिस्सा है, जिसका उद्देश्य आईटी सेवाओं में समस्याओं की पहचान, विश्लेषण, और समाधान करना है। यह प्रक्रिया घटना प्रबंधन (Incident Management) के बाद आती है और समस्याओं के मूल कारण को खोजने और उन्हें स्थायी रूप से हल करने पर केंद्रित होती है।

समस्या प्रबंधन के मुख्य उद्देश्य

1. समस्याओं की पहचानः सेवा में आई समस्याओं की पहचान करना और उन्हें रिकॉर्ड करना।
2. मूल कारण विश्लेषणः समस्याओं के पीछे के मूल कारणों का पता लगाना और विश्लेषण करना।
3. समाधान विकसित करनाः समस्याओं को हल करने के लिए स्थायी समाधान विकसित करना।
4. समस्याओं का निवारणः समस्याओं को प्रभावी ढंग से हल करना ताकि वे भविष्य में पुनरावृत्ति न हों।
5. दस्तावेजीकरणः सभी समस्याओं और उनके समाधानों को दस्तावेज़ित करना ताकि भविष्य में संदर्भ के लिए उपलब्ध हो।

अपनी प्रगति जांचें

अ. बहु विकल्पीय प्रश्न

1. ITIL की आवश्यकता क्यों है?

A. लागत में कमी B. सेवा की गुणवत्ता में सुधार

C. व्यावसायिक प्रक्रियाओं का अनुकूलन D. उपरोक्त सभी

2. ITIL के किस संस्करण को 2007 में जारी किया गया था?

A. ITIL v1 B. ITIL v2

C. ITIL v3 D. ITIL 4

3. ITIL प्रकाशनों में कौन सा प्रकाशन सेवा प्रबंधन के चार मूलभूत स्तंभों को कवर करता है?

A. सेवा रणनीति
B. सेवा डिजाइन
C. सेवा संक्रमण
D. उपरोक्त सभी

4. ITIL के कार्यान्वयन से निम्नलिखित में से क्या लाभ होता है?

A. सेवा की उपलब्धता में सुधार
B. संगठनात्मक उत्पादकता में कमी
C. ग्राहक संतोष में कमी
D. सभी का समावेश

5. ITIL v2 और ITIL v3 के बीच प्रमुख अंतर क्या है?

A. प्रक्रिया का विवरण
B. प्रक्रिया की संख्या
C. उपरोक्त दोनों
D. कोई अंतर नहीं

6. सेवा की अवधारणा का क्या अर्थ है?

A. उत्पाद का वितरण
B. ग्राहक की आवश्यकताओं को पूरा करने के लिए गतिविधियाँ
C. व्यवसाय का विस्तार
D. लागत में कमी

7. IT सेवा प्रबंधन (ITSM) का क्या उद्देश्य है?

A. केवल तकनीकी समस्याओं को हल करना
B. आईटी सेवाओं की गुणवत्ता को बढ़ाना
C. केवल ग्राहकों की शिकायतों का समाधान करना
D. केवल लागत को कम करना

SCERT DELHI

8. समस्या प्रबंधन का मुख्य उद्देश्य क्या है?

A. घटनाओं को रिकॉर्ड करना

B. समस्याओं के मूल कारणों की पहचान करना

C. सेवा स्तर को बढ़ाना

D. ग्राहक संतोष में कमी

9. ITIL के किस संस्करण में ग्राहक की अपेक्षाओं को ध्यान में रखा गया है?

A. ITIL v1 B. ITIL v2

C. ITIL v3 D. ITIL 4

10. ITIL के लाभों में से एक है:

A. तकनीकी ज्ञान की कमी

B. लागत में वृद्धि

C. ग्राहकों की संतोषजनकता में वृद्धि

D. कार्यक्षमता में कमी

ब. लघु उत्तरीय प्रश्न

1. ITIL की आवश्यकता क्यों महत्वपूर्ण है?
2. ITIL के मुख्य संस्करण कौन से हैं?
3. ITIL प्रकाशनों में कौन से प्रमुख दस्तावेज शामिल हैं?
4. ITIL के उपयोग के प्रमुख लाभ क्या हैं?
5. ITIL v2 और ITIL v3 में क्या प्रमुख अंतर है?

SCERT DELHI

नोट : इस पुस्तक में प्रयुक्त सामग्री एवं चित्र पूर्णतः शैक्षणिक उद्देश्य के लिए है, किसी व्यावसायिक उपयोग के लिए नहीं।

राज्य शैक्षिक अनुसंधान एवं प्रशिक्षण परिषद, दिल्ली
वरुण मार्ग, डिफेंस कॉलोनी, नई दिल्ली - 110025