


The Internet - 11.1




Enterprise Networking

Session 11
The Internet

V2.1

© NCC Education Limited, 2007

The Internet - 11.2




Objectives

- Define internet and Internet
- Describe the background to the development of the Internet
- Understand the organisations and mechanisms that guide the development of the Internet
- Recognise the role played by protocols, especially TCP/IP
- Describe the development of the World Wide Web
- Recognise future trends

V2.1

© NCC Education Limited, 2007

The Internet - 11.3



Definitions


An internet
An internet is a collection of packet switched networks interconnected by routers, using protocols that allow them to perform logically as one single network

The Internet
The Internet is a collection of networks and routers that span most countries and uses the TCP/IP protocol to form a single virtual network

V2.1

© NCC Education Limited, 2007

The Internet - 11.4




Characteristics of the Internet

- No single controlling authority
- The ability to grow without reaching artificial limits
- Spans most countries with a robust and universal computer network
- Utilises open standards
- Uses a packet switched connectionless approach
- Connected computers are termed 'hosts'
- Each host has a unique IP address
- Form of address is a.b.c.d where a to d are 8 Octet numbers between 0 and 255
- All hosts within a single network share a similar address

V2.1

© NCC Education Limited, 2007

The Internet - 11.5




Internet Protocols

- Defined by a series of documents termed Request For Comment (RFC)
- RFCs are publicly available
- New protocols developed in an open collaborative fashion
- When a protocol has completed its RFC stage it is assigned an STD number
- The most important and fundamental protocols are
 - Internet Protocol (IP)
 - Transmission Control Protocol (TCP)
 - User Datagram Protocol (UDP)
 - Domain Name System (DNS)

V2.1

© NCC Education Limited, 2007

The Internet - 11.6




IP Address Configurations

	0	1	2	3	4		8		16		24		31
Class A	0	NETID					HOSTID						
Class B	1	0	NETID				HOSTID						
Class C	1	1	0	NETID			HOSTID						

V2.1

© NCC Education Limited, 2007

The Internet - 11.7




Subnet Addressing (1)

- The success of IP is causing a shortage of addresses
- NETID and HOSTID is too coarse
- A single business may need three class C networks leaving a lot of addresses unusable
- Solution is to divide one class C network into 3 sub networks

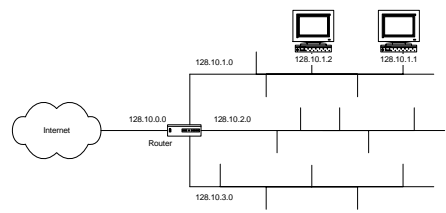
V2.1 © NCC Education Limited, 2007

The Internet - 11.8




Subnet Addressing (2)

- Subnet masks are used to separate the part of the address which is used for the host
- Mask is expressed in dotted quad format (255.255.255.0)



V2.1 © NCC Education Limited, 2007

The Internet - 11.9




IP and Ethernet

- When TCP/IP is used in a LAN, physical addresses have to be mapped to IP addresses
- The physical address with Ethernet is 48 bits
- To communicate with a host a PC needs to obtain the Ethernet address from the IP address
- Process is undertaken using Address Resolution Protocol (ARP)
- Message asks host with required IP address to respond with physical address
- Only host with required IP address responds
- Once host knows the destination address it is retained in a cache

V2.1 © NCC Education Limited, 2007

The Internet - 11.10




DHCP

- Hosts that are not permanently connected to the Internet often do not have a static IP address
- DHCP used to dynamically assign an address
- Special server assigns IP addresses to hosts that request one
- IP addresses may be leased to a host for a fixed time period

V2.1 © NCC Education Limited, 2007

The Internet - 11.11




The IP Datagram

- Data is conveyed in a datagram
- Datagram consists of header data followed by data payload

V2.1 © NCC Education Limited, 2007

The Internet - 11.12




The IP Format

VER	HLEN	SERVICE TYPE		TOTAL LENGTH											
IDENTIFICATION										DF	MF	FRAGMENT OFFSET			
TIME TO LIVE				PROTOCOL				HEADER CHECKSUM							
SOURCE ADDRESS															
DESTINATION ADDRESS															
IP OPTIONS															
DATA...															

V2.1 © NCC Education Limited, 2007

The Internet - 11.13




Internet Protocol version 6 (IPv6)

- Also called Next Generation Internet Protocol or IPng
- Developed in response to limited number of current IP addresses
- Installed as a software upgrade in Internet devices
- Designed to run on high performance networks
- Provides a platform for future Internet functionality

V2.1 © NCC Education Limited, 2007

The Internet - 11.14




IPv6 Changes

- Expanded routing and addressing capabilities
- New type of address – ‘anycast address’
- Header format simplification
- Improved support for IP header options
- Enhanced quality-of-service capabilities
- Authentication and privacy capabilities

V2.1 © NCC Education Limited, 2007

The Internet - 11.15




IPv6 Header Format

- Version – 4-bit Internet Protocol version number 6
- Priority – 4-bit priority value
- Flow Label – 24-bit field
- Payload Length – 16-bit unsigned integer
- Next Header – 8-bit selector
- Hop Limit – 8-bit unsigned integer
- Source Address – 128-bits
- Destination Address – 128 bits

V2.1 © NCC Education Limited, 2007

The Internet - 11.16




IPv6 Extension Headers

Currently defined:

- Routing
- Fragmentation
- Authentication
- Encapsulation
- Hop-by-hop options
- Destination options

V2.1 © NCC Education Limited, 2007

The Internet - 11.17




IPv6 – Next Generation

- Solves Internet scaling problems
- Provides flexible transition mechanism for current Internet
- Designed to meet the needs of new markets
- Evolutionary approach reduces the risk of architectural problems

V2.1 © NCC Education Limited, 2007

The Internet - 11.18



Transmission Control Protocol (TCP)

- Operates on top of IP to produce reliable data transmission from one host to another
- Breaks data into packet sized chunks
- Reassembles chunks at destination
- Reliability is ensured by using checksum
- Corrupted packets are instructed to be re-sent
- A replacement will be requested for missing packets

V2.1 © NCC Education Limited, 2007

TCP Transmission

- A connection to each host is through a 'port'
- Port pairs are identified by their hosts' IP addresses
- Addresses need not be different
- Messages are associated with a connection
- A connection is defined by a pair of address end points

TCP Format

The diagram illustrates the structure of a TCP header. It starts with a 32-bit field for the source port, followed by another 32-bit field for the destination port. This is followed by 32-bit fields for the sequence number and the acknowledgement number. A 4-bit field for 'TCP HLEN' is shown, followed by a 2-bit 'URG' flag, a 2-bit 'ACK' flag, a 2-bit 'PUSH' flag, a 2-bit 'RESET' flag, and a 2-bit 'FIN' flag. A 16-bit 'WINDOW SIZE' field follows. Then come 16-bit fields for 'CHECKSUM' and 'URGENT POINTER'. An 'OPTIONS' field of 0 or more 32-bit words is shown, followed by a 'DATA (optional)' section.

User Datagram Protocol (UDP)

- Operates on top of IP
- Avoids complications of TCP
- Does not have same capability as TCP to ensure reliability
- Lost packets will not be corrected by UDP

UDP Format

The diagram shows the UDP header structure. A double-headed arrow at the top indicates a total width of 32 bits for the header fields. Below this, there are four 16-bit fields: 'Source port', 'Destination port', 'Length', and 'Checksum'. Below these fields is a larger section for 'Data (variable number of octets)'.


Domain Name System (DNS)

- DNS overcomes the inconvenience of totally numeric addresses
- Textual name allocated in lieu of numeric address
- Name built up by using words separated by dots e.g www.ncceducation.co.uk
- Example shows www hosts belonging to ncceducation domain, belonging to company domain, belonging to UK domain
- Popular implementation is through UNIX program Berkeley Internet Name Domain (BIND)

Windows Internet Naming Service (WINS)

- Can be used in networks containing Windows clients and Windows NT servers
- Provides some functionality needed to map host names to IP addresses
- Main usage maps names with NetBIOS and NetBUI
- With later versions of Windows WINS is not necessary as TCP/IP is default network protocol using DNS
- Not suitable for large networks

The Internet - 11.25




Routing

- IP uses packet switched connectionless approach
- Routers have to decide what to do with a packet based on the address data in the packet header
- Potential delay precludes complex processing
- Network quantities preclude each router 'knowing' all routes
- Table-driven approach used with each router only identifying next hop
- Router only needs to recognise non 'home' packets
- Allows manual construction of routing tables for small networks
- Large networks need an automated process for creating tables

V2.1 © NCC Education Limited, 2007

The Internet - 11.26




Routing Protocols

- Standard interior gateway protocol is Open Shortest Path First (OSPF)
- Standard exterior routing protocol is Border Gateway Protocol (BGP)

V2.1 © NCC Education Limited, 2007

The Internet - 11.27




Internet Diagnostics

- Wide range of tools available:
 - PING – to test whether it is possible to reach a host
 - TRACEROUTE – shows what networks are traversed
 - NSLOOKUP – tests ability of DNS to resolve a domain name

V2.1 © NCC Education Limited, 2007

The Internet - 11.28




Internet Administration

- Internet not 'owned' by anyone
- Internet Society (ISOC) concerned with political and social development
- Internet Architecture Board (IAB) technical advisory group within ISOC
- Internet Engineering Steering Group (IESG) technical management responsible for Internet Standards
- Internet Engineering Task Force (IETF) informal group contributing to Internet development at a technical level. Makes recommendation to IESG
- Internet Research Task Force (IRTF) long-term research

V2.1 © NCC Education Limited, 2007

The Internet - 11.29




ISOC

- Non-profit, non-government, international professional organisation
- More than 8,600 individual members across 170 nations
- Focuses on standards, public policy, education, training and membership

V2.1 © NCC Education Limited, 2007

The Internet - 11.30




IETF

- Consists of international network designers, operators, vendors and researchers
- Concerned with evolution of the Internet
- Open to any interested individual
- Work is undertaken in technical working groups

V2.1 © NCC Education Limited, 2007

The Internet - 11.31




International Assigned Number Authority (IANA)

- Central co-ordinator for the assignment of unique parameter values for Internet protocols
- Acts as a clearing house to assign and co-ordinate the use of numerous Internet protocol parameters

V2.1 © NCC Education Limited, 2007

The Internet - 11.32




International Architecture Board (IAB)

- Technical advisory group of ISOC
- Selection of chairmen of other organisations such as IESG
- Architectural oversight of protocols and procedures
- Standards process oversight
- Editorial management of Request For Comment (RFC)
- External liaison with non-Internet organisations

V2.1 © NCC Education Limited, 2007

The Internet - 11.33




Internet Corporation for Assigned Names and Numbers (ICANN)

- Responsible for managing and co-ordinating the Domain Name System (DNS)
- Oversees the distribution of unique IP addresses and domain names
- Ensures each domain name maps to the correct IP address
- Responsible for accrediting domain name registrars

V2.1 © NCC Education Limited, 2007

The Internet - 11.34




Internet Applications

- Electronic Mail (Email)
- File transfer (FTP)
- Remote login (TELNET)
- Newsgroups
- World Wide Web (www)

V2.1 © NCC Education Limited, 2007

The Internet - 11.35




Email

- Sending messages from one Internet user to another using Internet as delivery mechanism
- Store and forward approach
- Progression from sender to receiver in series of hops from host to host
- Relies on use of unified addressing structure consisting of:
 - domain name (ncceducation)
 - user name (joe)
 - separated by an @sign (joe@ncceducation.co.uk)

V2.1 © NCC Education Limited, 2007

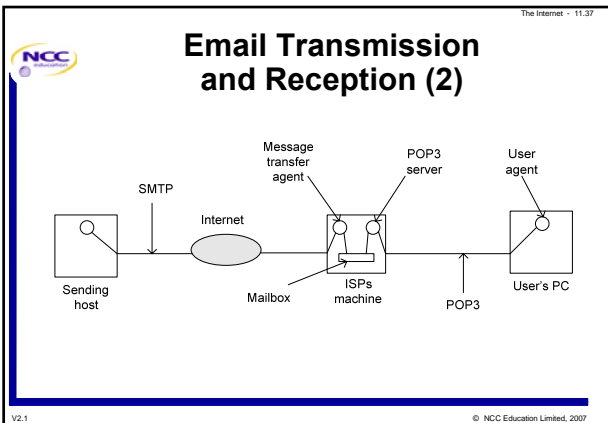
The Internet - 11.36



Email Transmission and Reception (1)

- Transmission defined by Simple Mail Transfer Protocol (SMTP)
- Reception defined by Post Office Protocol (POP3)
- Designed for 7-bit ASCII text only
- Many messages originate in 8-bit format
- Conversion from 8-bit to 7-bit is carried out by Multipurpose Internet Mail Extension (MIME)
- Compliance with MIME allows 8-bit message attachments

V2.1 © NCC Education Limited, 2007



File Transfer Protocol (FTP)

- Used to simplify copying of files from one computer to another
- Also used to retrieve file from Internet archives
- Offers different ways to transfer files dependent upon their content
- Needs a login procedure to gain access to remote host
- To allow access to Internet archives, an Anonymous FTP is used where user name is 'anonymous' and their email address is the password

Telnet

- Remote login to another host
- Uses client/server approach
- Telnet client is program that the users run at their workstation
- Server is remote machine
- Typical emulations are DEC VT100 or IBM 3270
- Use of a user name and password is essential

World Wide Web (1)

- Concept devised by Tim Berners-Lee while working at CERN
- Hypertext is text that contains references to other documents
- User can use references to call up other documents
- Hypermedia is a further development of hypertext
- Brings together several Internet protocols in a common fashion
- Unified protocols include:
 - Telnet
 - Ftp
 - Newsgroups
 - Wide Area Information Servers (WAIS) for searching indexes
 - Gopher for browsing Internet resources


World Wide Web (2)

- Browser used to read web pages and recognises other document references
- HyperText Transfer Protocol (HTTP) is used to define how a browser issues requests to the web server and how the web server is intended to respond
- Web pages are written in HyperText Markup Language (HTML) or other language

HTTP

- Used throughout the World Wide Web
- All clients and servers must obey this protocol
- Has a number of methods:
 - GET - request the server to send a page
 - HEAD - request a web page's header
 - PUT - store a page on a server
 - POST - append data to a page
 - DELETE - remove a web page
 - TRACE - return the request

The Internet - 11.43




HTTP Status Codes

Code	Meaning	Information/Example
1xx	Information	Rarely used 100 = server agrees to handle request
2xx	Success	200 = request succeeded
3xx	Redirection	301 = page moved
4xx	Client error	403 = forbidden page
5xx	Server error	500 = internal server error

V2.1 © NCC Education Limited, 2007

The Internet - 11.44




HTML

- Markup language that describes how documents are to be formatted
- Standardising and embedding markup commands within each file allows browser to read and reformat any page

V2.1 © NCC Education Limited, 2007

The Internet - 11.45




XML and XSL

- XML has a defined structure allowing for great detail to be stored in very simple ways that are machine readable
- XSL is the related language used to store the information on how to display the XML file on screen
- XML is also used for communicating between applications as it is language and system independent

V2.1 © NCC Education Limited, 2007

The Internet - 11.46




XHTML

- More rigorous than HTML
- Pages and browsers must strictly conform to the standard
- Aids the reading of web pages by portable devices
- HTML and XHTML when used alone produce *static* web pages

V2.1 © NCC Education Limited, 2007

The Internet - 11.47




Dynamic Web Pages

- Content is generated on demand
- Server-side dynamic web page generation typically has a server-side script to perform some function based upon user-supplied information
 - Perl
 - PHP
 - JSP
 - ASP
- Client-side dynamic web pages can interact directly with user events
 - JavaScript
 - Java Applets
 - ActiveX

V2.1 © NCC Education Limited, 2007

The Internet - 11.48




WWW Architecture and Components

- User can navigate a network (the Web) by using references
- Resources can be located on any machine linked to the Internet
- Each resource is identified by a Uniform Resource Locator (URL) which defines how the resource can be found
- WWW servers receive requests for URLs from browsers and perform one of the following actions:
 - translate URL into a file name or a location in a file and send back that file to the browser
 - translate the URL into a program name which is run, sending the output back into the browser

V2.1 © NCC Education Limited, 2007

The Internet - 11.49




Uniform Resource Locators

- Made up of two parts
 - scheme
 - scheme-specific-part
- Scheme is protocol used by user – ftp, http, gopher, mailto, news, nntp, telnet, wais, file, prospero
- Only ftp, http and file are in common use
- Scheme specific part is made up of the following:
 - //<user>:<password>@<host>:<port>/<url-path>
- // indicates what follows is Internet specific scheme part
- <user>:<password>@ and <port> can be omitted
- The <host> part can be the fully qualified domain name of the network host or its IP address e.g.
 - www.ncceducation.co.uk or 195.102.153.3

V2.1 © NCC Education Limited, 2007

The Internet - 11.50




Other Internet Applications

- Voice over IP (VoIP)
 - needs voice signals to be digitised
 - needs resultant digital signals to be packetised
 - packets may be sent by different routes
 - packets must be re-assembled to form continuous audio waveform with accurate timing and no gaps
 - result must be an acceptable reproduction of original audio signal

V2.1 © NCC Education Limited, 2007

The Internet - 11.51




VoIP via the Internet

- Inadequate capacity requires compression of voice signals
- Compression can disrupt quality
- Cost advantage because of local call cost of accessing Internet
- Needs a local Gateway to allow Internet to originate telephone calls
- Wholesale VoIP over present day Internet is unlikely to be economically viable
- VoIP over a high capacity digital network will be a viable economic proposition

V2.1 © NCC Education Limited, 2007

The Internet - 11.52




Web Services

- Share business logic, data and processes across a network via a programmatic interface
- Applications that reside on a server without a user interface and provide objects to clients
- Combine four standards:
 - XML is used to tag the data
 - SOAP to transport the data
 - WSDL to describe the data
 - UDDI to list the available services

V2.1 © NCC Education Limited, 2007

Network Management - 12.1




Enterprise Networking

Session 12
Network Management

V2.0 © NCC Education Limited, 2004

Network Management - 12.2




Objectives

- Appreciate the nuances of network management
- Understand why network management is important to
 - network users
 - network operators

V2.0 © NCC Education Limited, 2004

Network Management - 12.3




Important Issues of Network Management

- After failure, how quickly can the network be restored
- Minimisation of operational costs by
 - reducing operation staff quantities
 - de-skilling the role of support staff
 - ensuring peak performance commensurate with required need

V2.0 © NCC Education Limited, 2004

Network Management - 12.4




Importance of Network Definition

- Individual's perception of a network varies
- A computer expert's view of a network will not be the same as a telecommunications expert
- Difference of view probably stems from the network's perceived functionality

V2.0 © NCC Education Limited, 2004

Network Management - 12.5




Important Aspects of Network Operation

- Preferably the network should be operational at all times
- If the network becomes unoperational it should be restored to service in shortest possible time
- To achieve the above it is necessary to
 - monitor the network's performance
 - take remedial action when any performance parameters move outside set values

V2.0 © NCC Education Limited, 2004

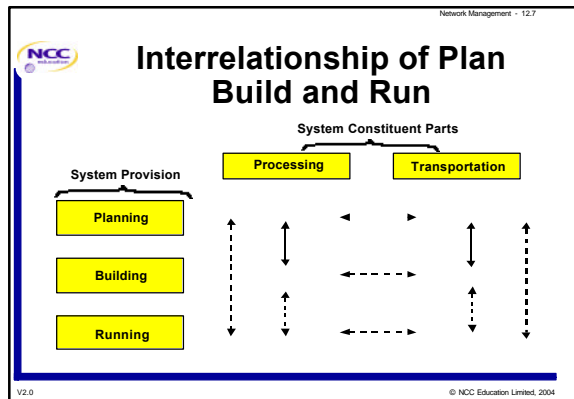
Network Management - 12.6



Operation and Planning Processes

- All projects consist of three phases
 - planning
 - building
 - running

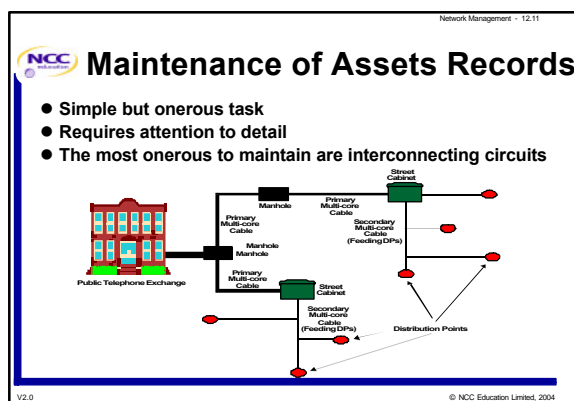
V2.0 © NCC Education Limited, 2004



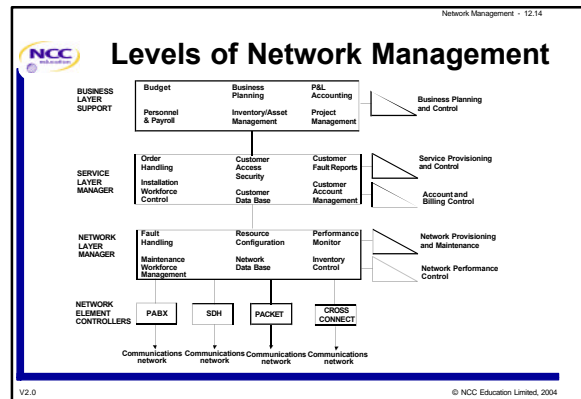
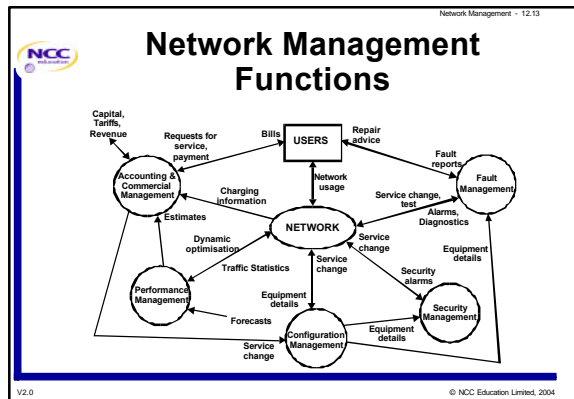
- Network Management - 12.8
- Network Asset Management**
- Alternative views of assets
 - substantial capital outlay
 - to recoup investment, network must be operational
 - In relation to the above, operators must keep track of assets to assess:
 - how they are affecting network performance
 - how they can be exploited
- V2.0 © NCC Education Limited, 2004

- Network Management - 12.9
- Identifying Assets**
- Network assets consist of
 - interconnecting circuits
 - interconnecting equipment
 - planning, building and running staff
 - Local Area Networks may differ from wide area networks
- V2.0 © NCC Education Limited, 2004

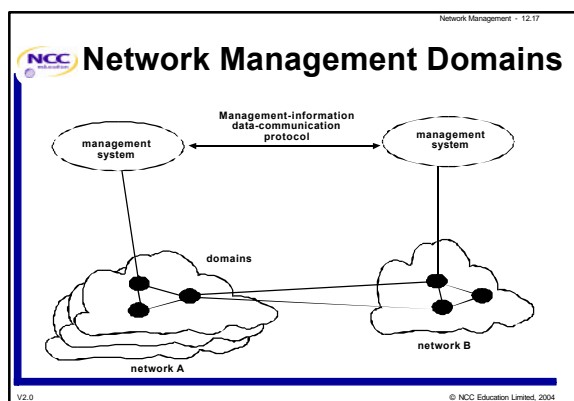
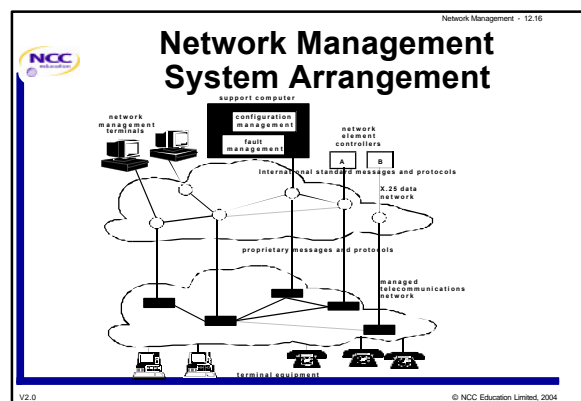
- Network Management - 12.10
- Key Factors in the Management of Assets**
- Maintaining records of all constituent network parts whether used or not
 - Ensuring constituent parts cannot be interfered with either deliberately or accidentally
 - When disruption occurs, restore network services as soon as possible
- V2.0 © NCC Education Limited, 2004



- Network Management - 12.12
- The Operator's View of Network Management**
- Ensuring costs are kept to a minimum
 - Ensuring management systems themselves are reliable
- V2.0 © NCC Education Limited, 2004




- Network Management - 12.15
- ### Network Management System Architecture
- Operations language
 - Management terminals
 - Application software
 - Support computers
 - A network for network management communications
 - A language for the network
 - Network element management controllers
 - Network elements
- V2.0 © NCC Education Limited, 2004



- Network Management - 12.18
- ### Applications Software and Support Computers
- System will be multifunctional
 - Applications will be software implemented
 - A set of core functions should meet the majority of needs
 - Core functions should be customised to provide specialist needs
- V2.0 © NCC Education Limited, 2004

Network Management - 12.19




Fault Management

- An essential part of network management
- Needs to cover
 - detection of faults
 - diagnosis
 - isolation
 - correction of abnormal operations
 - maintenance work tracking

V2.0 © NCC Education Limited, 2004

Network Management - 12.20




Configuration and Name Management

- Needed to keep track of all resources
- Master database must remain in step with all changes
- Functions to be covered include
 - Equipment number/directory number mapping
 - Identity, status and position of every network element
 - Interconnection details of elements
 - Routing table contents
 - Writing of mapping rules

V2.0 © NCC Education Limited, 2004

Network Management - 12.21




Accounting and Commercial Management

- Means to support sales of services
- Management of accounts and billing
- Maintenance of user records
- Financial control of installed system

V2.0 © NCC Education Limited, 2004

Network Management - 12.22




Performance Management

- Collecting traffic statistics
- Determining correlation between nodes
- Analysing traffic flows

V2.0 © NCC Education Limited, 2004

Network Management - 12.23




Security Management

- Who may do what, where, how and when
- Access methods:
 - passive (read only)
 - active (read and write)
 - command (executive operation)

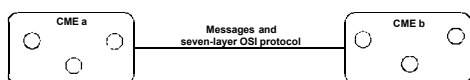
V2.0 © NCC Education Limited, 2004

Network Management - 12.24



Network Management Communications Language

- Many systems exist that use a variety of languages
- Many use the Simple Network Management Protocol (SNMP) for TCP/IP networks
- Network Management Forum have produced a simple architecture




```

            graph LR
            CMEa[CME a] ---|Messages and seven-layer OSI protocol| CMEb[CME b]
            
```

CME = Conformant Management Entity

V2.0 © NCC Education Limited, 2004

Network Management - 12.25




Network Management Communications Network

- Can be either separate overlay network or the network that is being managed
- In large networks the traffic generated by management will necessitate a separate network

V2.0 © NCC Education Limited, 2004

Network Management - 12.26




Network-Element Controller Functions

- Remote sites will store data
- Significant data needs to be sent to central management system
- Centralised control information needs to be distributed to remote sites

V2.0 © NCC Education Limited, 2004

Network Management - 12.27




Network Elements

- Many and various
- All must provide a control and monitoring interface for:
 - control state
 - monitoring quality of operation
 - monitoring usage of network

V2.0 © NCC Education Limited, 2004

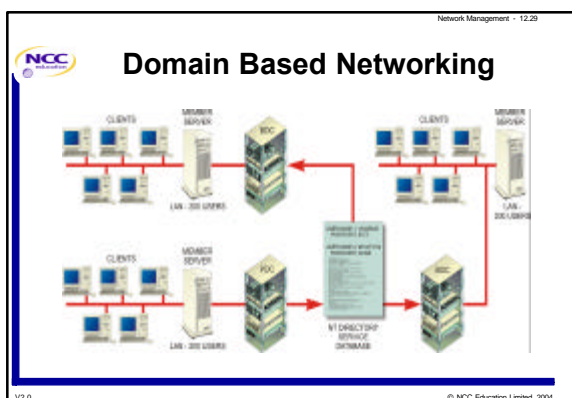
Network Management - 12.28




Operational and Maintenance Instructions

- Only source of information as to how the various network elements should function
- Maintenance of manuals is a vitally important function
- Hard copy versions are subject to wear and tear
- Opportunity to become familiar with contents is limited
- Can consist of many volumes covering many and varied procedures
- Online versions, which can automate presentation of text and diagrams, are most useful

V2.0 © NCC Education Limited, 2004



Network Management - 12.30




Characteristics of Domain Based Networking

- Network controlled from a centralised server
 - Windows NT has primary domain controllers (PDCs) and backup domain controllers (BDCs)
- System of managing access to distributed data must be implemented
 - Windows 2000 has feature called Active Directory (AD)
 - Helps to centralise system and user configurations

V2.0 © NCC Education Limited, 2004

Customer Premise Equipment - 13.1




Enterprise Networking

Session 13
Customer Premise Equipment

V2.1 © NCC Education Limited, 2007

Customer Premise Equipment - 13.2




Objectives

- Describe the main equipment or systems likely to be adopted by users for connection to public telecommunications networks
- Understand
 - the functions of PBXs and KTSs
 - call centre functions
 - the meaning of voice processing and the systems which use it
 - the basic functionality of call information loggers and facsimile

V2.1 © NCC Education Limited, 2007

Customer Premise Equipment - 13.3




Basic Functions of a Telephone Instrument

- Provide a signal on call receipt
- Signal to the exchange a need for call origination
- Permit the user to advise the exchange the number required
- Advise the exchange when a call has finished
- Convert voice signals to varying electrical signals and vice versa
- Receive voice signals in preparation for conversion

V2.1 © NCC Education Limited, 2007

Customer Premise Equipment - 13.4




Private Branch Exchange (PBX)

- Connects any internal extension to any external line
- Allows internal extensions to connect to each other

V2.1 © NCC Education Limited, 2007

Customer Premise Equipment - 13.5




Key Telephone System (KTS)

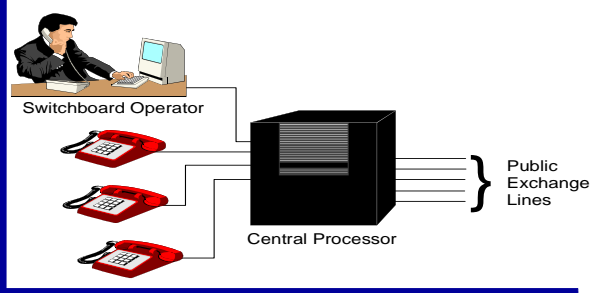
- Provides all of the functions of a PBX
- Provide a more economic alternative to a PBX for smaller installations

V2.1 © NCC Education Limited, 2007

Customer Premise Equipment - 13.6

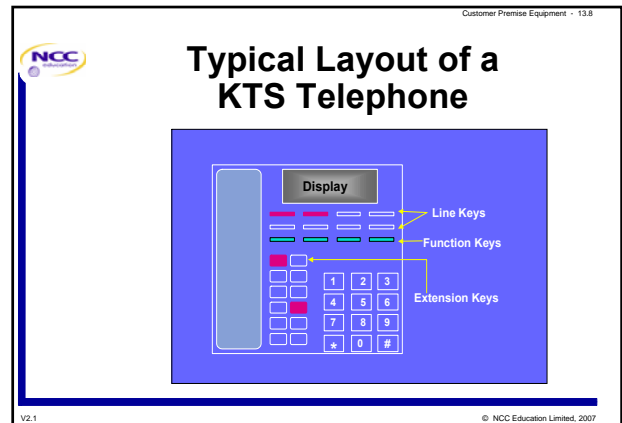
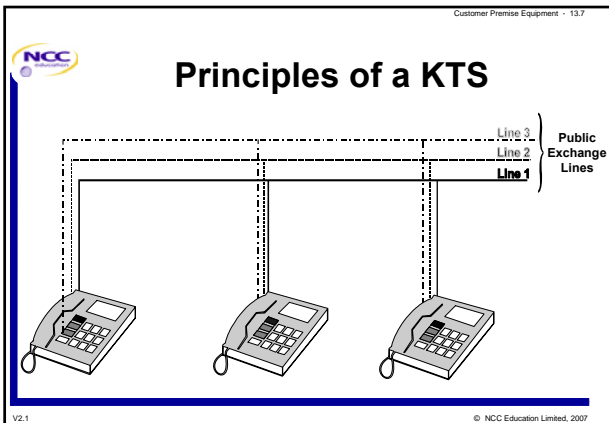


Principles of a PBX



The diagram illustrates the components of a PBX system. On the left, a **Switchboard Operator** is seated at a desk with a computer monitor. Below the operator are three red telephones. Lines connect the operator and the telephones to a central **Central Processor** unit. From the right side of the central processor, lines extend to a bracketed area labeled **Public Exchange Lines**.

V2.1 © NCC Education Limited, 2007

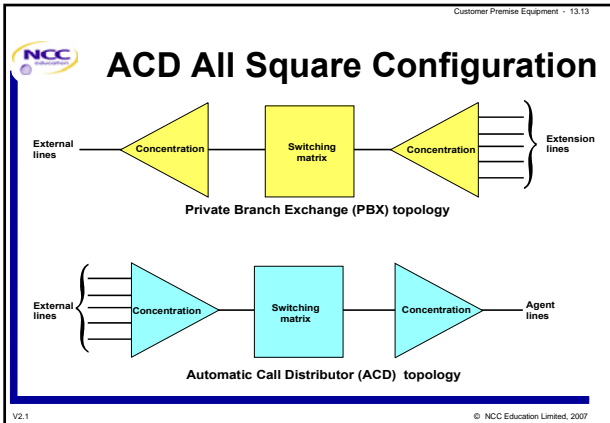


- ### Differences Between a KTS and PBX
- KTS do not have a central processor
 - PBXs are more economic for larger installations
 - KTS user selects external line
 - PBX system selects external lines
 - KTS do not have a switchboard console

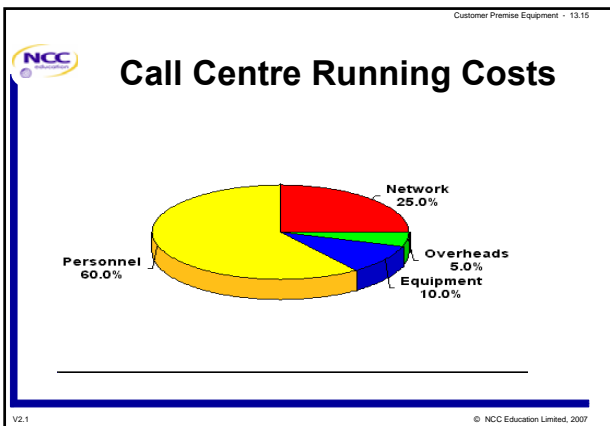
- ### KTS and PBX Basic System Features
- To allow extension users to
 - dial other extensions
 - dial external lines
 - receive external calls
 - make an enquiry call to another extension
 - transfer a call to another extension

- ### KTS and PBX Advanced User Features
- Call barring – prevention of calls
 - Hunt groups – one number selects a group of lines
 - Call diversion – calls sent to another extension
 - Short code dialling
 - Night service – handling of out-of-hours calls
 - Call parking – to enable a call to be picked up at another location
 - Call hold – to avoid caller overhearing
 - Automatic call back – also know as 'Call back when free'
 - Conference call – a number of telephones connected to one line
 - Communications group – a department with a close community of interest
 - Automatic answers – avoids having to lift handset, poses a security risk
 - Temporary barring of external calls
 - Save last number dialled

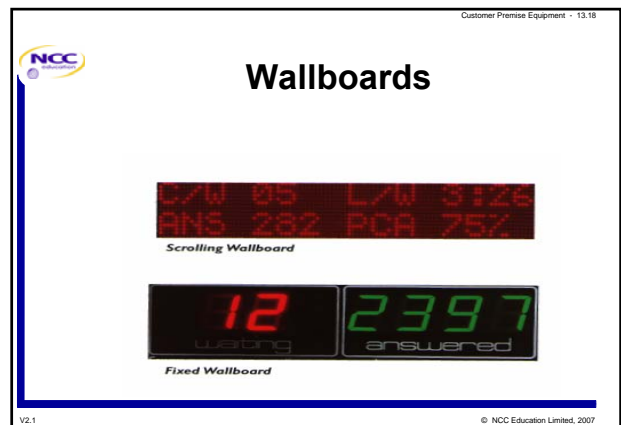
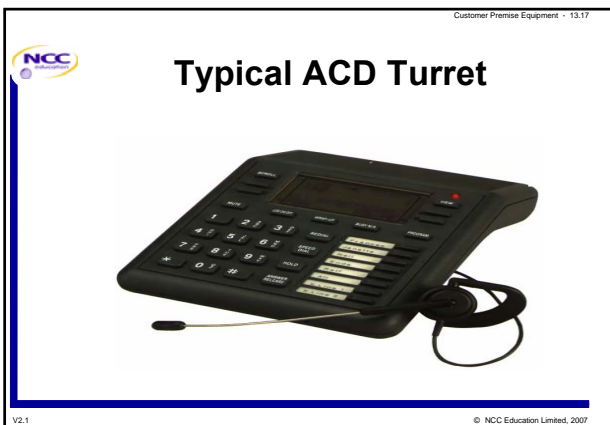
- ### Automatic Call Distribution (ACD)
- Designed to improve the handling of intensive call quantities
 - Not good at distributing calls
 - Best when call answerer handles call entirely
 - Produces comprehensive real-time statistics



- Customer Premise Equipment - 13.14
- ### Call Centres
- Need a telephone system – PBX or Automatic Call Distribution system
 - May be associated with a computer system – Computer/Telephony Integration (CTI)
 - Used for intensive call handling
 - Used to improve a caller's or called person service
 - All calls must have the same or similar characteristics
 - All calls can be handled by any one of a group of answerers
 - The call answerer deals with the call
 - Often confused with a call distributor
- V2.1 © NCC Education Limited, 2007



- Customer Premise Equipment - 13.16
- ### Call Centre Popularity
- The telephone is simple to use
 - Telephone technology does not overawe users
 - All age groups are familiar with the telephone
 - Most social classes are familiar with the telephone
 - The telephone allows person-to-person communications
- V2.1 © NCC Education Limited, 2007



Customer Premise Equipment - 13.19

Computer Telephony Integration (CTI)

- Telephone system supplies information to computer system
- Computer system controls telephone system

V2.1 © NCC Education Limited, 2007

Customer Premise Equipment - 13.20

CTI Developments

- Production of Application Programming Interfaces (API)
 - Microsoft’s Telephony API (TAPI)
 - Novell’s Telephone Service API (TSAPI)
 - IBM’s Callpath
- Increasing use of Calling Line Identification and Direct Dialling-In to personalise service

V2.1 © NCC Education Limited, 2007

Customer Premise Equipment - 13.21

Voice Processing Systems

- Voice messaging
- Automatic attendant
- Interactive Voice Response (IVR)

V2.1 © NCC Education Limited, 2007

Customer Premise Equipment - 13.22

Voice Messaging

- Each extension user is allocated a mailbox
- Callers enter mailbox if extension user is absent
- Mailbox owner can customise greeting
- Mailbox owner gets indication of deposited message
- More sophisticated systems can deliver message
- More sophisticated systems can be linked to email

V2.1 © NCC Education Limited, 2007

Customer Premise Equipment - 13.23

Voice Messaging System Configuration

V2.1 © NCC Education Limited, 2007


Customer Premise Equipment - 13.24

Automatic Attendant

- Answers incoming calls within a pre-determined time
- Places caller in a queue and advises them of position
- Allows Direct Inward System Access (DISA)
- Poor substitute for an efficient answering service
- Can save on switchboard operator costs
- Very useful out of normal hours

V2.1 © NCC Education Limited, 2007

Customer Premise Equipment - 13.25




Interactive Voice Response (IVR)

- Used to automate simple administrative tasks
- May be unpopular with casual callers
- Requires verbal input
- Requires tone (DTMF) input

DTMF = Dual Tone Multi Frequency

V2.1 © NCC Education Limited, 2007

Customer Premise Equipment - 13.26




Call Logging Systems

- Receive call records from PBX consisting of
 - Extension number making call
 - Number dialled
 - Date and time
 - Duration of call
- Manipulate information to provide system usage reports

V2.1 © NCC Education Limited, 2007

Customer Premise Equipment - 13.27




Typical Call Logger Reports

- All calls over 2 minutes
- All calls over \$5
- 20 most dialled numbers
- Total cost per department per month
- Total site cost per month
- All calls for all extensions

V2.1 © NCC Education Limited, 2007

Customer Premise Equipment - 13.28




Facsimile

- Can transmit text and graphics over PSTN
- First machines were in use in the 1940s
- Scans pages looking for black and white
- Converts black and white to analogue tones
- Four groups (1 to 4) available
- Group 3 maximum speed is 9.6 Kbits/s
- Group 4 is digital and runs at 64 Kbits/s
- Uses thermal or plain paper

V2.1 © NCC Education Limited, 2007

Customer Premise Equipment - 13.29




Digital Enhanced Cordless Telecommunications (DECT)

- Radio technology suited for voice and multimedia traffic
- Used for Internet access and internetworking
- Incorporates encryption for call security
- DECT standard makes use of advanced techniques
 - TDMA (Time Division Multiple Access)
 - ADPCM (Adaptive Differential Pulse Code Modulation)
 - DCS/DCA (Dynamic Channel Selection/Allocation)

V2.1 © NCC Education Limited, 2007

Within Site Networks - 143




Enterprise Networking

Session 14
Within Site Networks

V2.0 © NCC Education Limited, 2004

Within Site Networks - 142




Objectives

- List the characteristics of a LAN and how it differs from a WAN
- Describe various types of physical network cabling used for LANs
- Understand the history and current approach to LAN cabling
- Recognise advantages of structured cabling
- Define the advantages and disadvantages of fibre optics
- Describe
 - Ethernet and its standards
 - Token ring and its standards
 - FDDI and its applications
- Define trends in LAN technology

V2.0 © NCC Education Limited, 2004

Within Site Networks - 143




Differences Between LANs and WANs

- LANs are limited in size
- WANs have less nodes than LANs
- LANs can use physical cable
- LANs can have lower error rates
- The usage limitation (single business) offers a wider choice of topology
- LANs are standard driven

V2.0 © NCC Education Limited, 2004

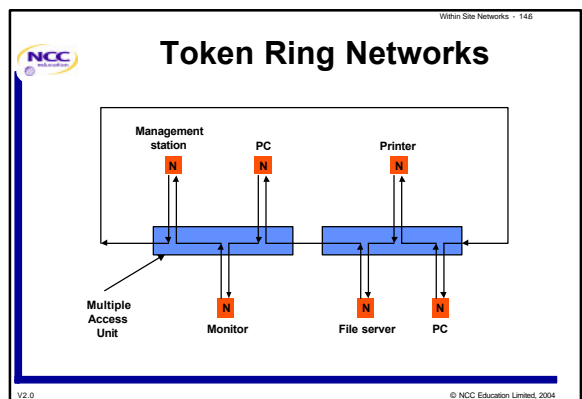
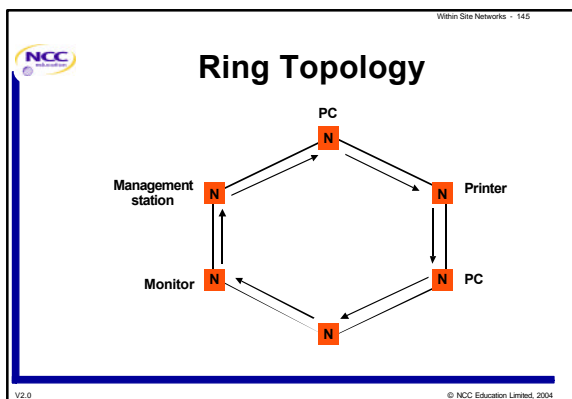
Within Site Networks - 144

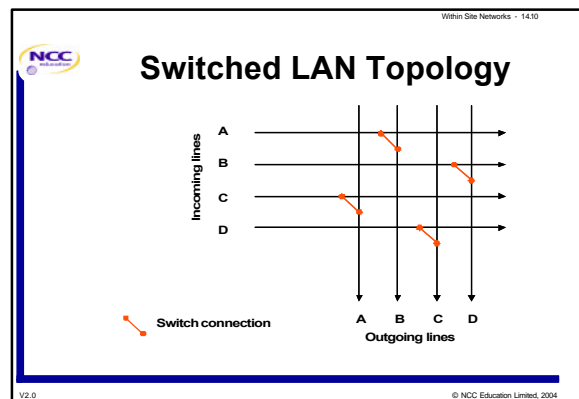
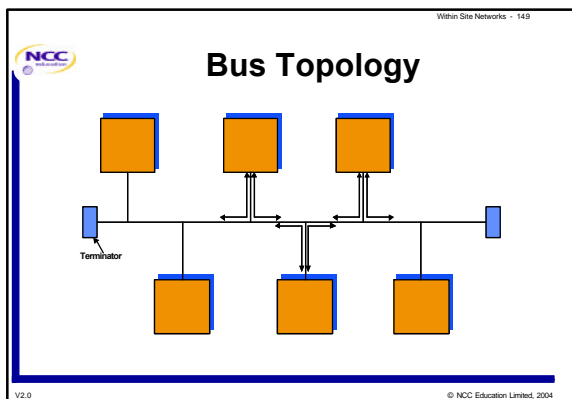
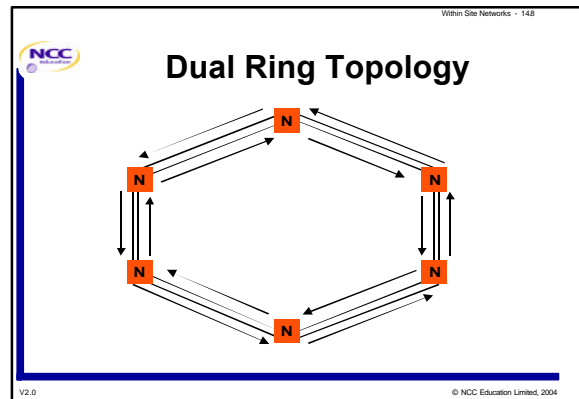
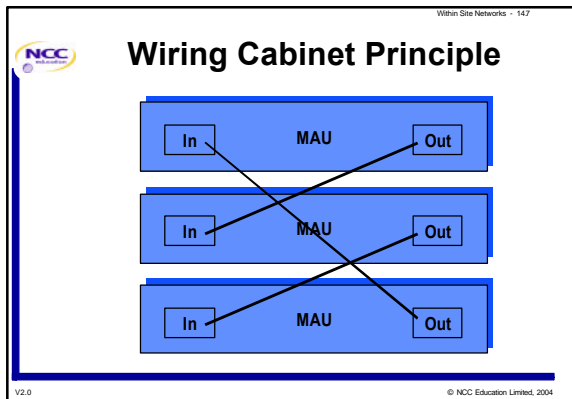


LAN Topology

- The logical and physical relationship between nodes
- Two logical topologies
 - Ring
 - Bus

V2.0 © NCC Education Limited, 2004





Within Site Networks - 1411

Network Access

- A node may wish to transmit data to any other node at any time
- Unless a discipline is imposed transmission attempts may clash
- Techniques used include:
 - Non-contention
 - Slotted access
 - Contention

V2.0 © NCC Education Limited, 2004


Within Site Networks - 1412

Non Contention Technique

- Designed to ensure no transmission conflicts
- Nodes are given exclusive opportunities to transmit
- Most important technique used is token passing
- Token passing is normally associated with ring topology
- Each node receives the right to transmit by the presence of a vacant token
- Token is a special packet that circulates from node to node

V2.0 © NCC Education Limited, 2004

Within Site Networks - 14.13




Slotted Access Technique

- Another form of token passing used primarily with ring topologies
- A number of 'slots' (dataframes) circulate
- A node wishing to transmit:
 - waits for a free slot
 - inserts data into the appropriate field
 - sets the destination and origination addresses
 - sets a bit value to indicate that the frame is in use
- Intermediate nodes check if the frame is addressed to them and, if not, repeats the frame
- Destination node:
 - copies the information from the slot
 - sets the appropriate bit value to indicate that the slot is empty

V2.0 © NCC Education Limited, 2004

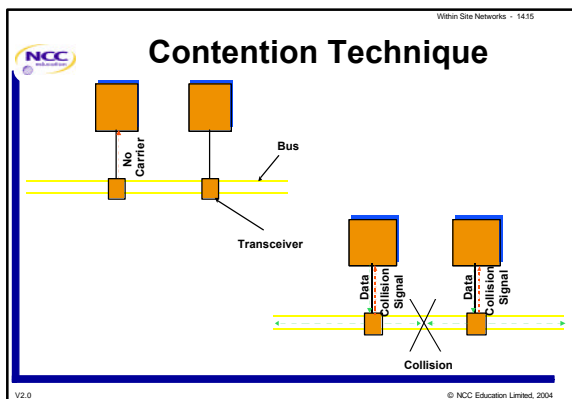
Within Site Networks - 14.14




Contention Technique

- Anticipates packet conflicts and collisions
- Any node can transmit at any time
- Most important technique used is Carrier Sense Multiple Access with Collision Detection (CSMA/CD)
- CSMA/CD allows a node to transmit a message when the network is free
- When two nodes detect a free network simultaneously a collision results

V2.0 © NCC Education Limited, 2004



Within Site Networks - 14.16




Media used for LANs

- Coaxial copper wire cable
- Twisted pair copper wire cable
- Optical fibre cable
- Radio
- A combination of all of the above

V2.0 © NCC Education Limited, 2004

Within Site Networks - 14.17




Coaxial Copper Wire Cable

- Known as
 - Coaxial cable
 - 10Base5 (Thick wire Ethernet)
 - 10Base2 (Thin wire Ethernet)

V2.0 © NCC Education Limited, 2004

Within Site Networks - 14.18




Twisted Pair Copper Wire Cable

- Known as
 - 10BaseT
 - Unshielded twisted pair
 - Shielded twisted pair
 - Category 5 or 5e or 6

V2.0 © NCC Education Limited, 2004

Within Site Networks - 1419




Optical Fibre Cable

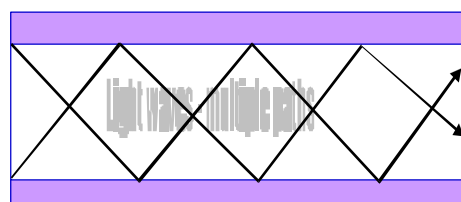
- Immune to electrical interference
- Capable of covering large areas
- Very high transmission speeds (>1,000 Mbits/s)
- Cannot easily be intruded upon
- Most popularly used as backbone for a large LAN
- Multimode and Monomode operation

V2.0 © NCC Education Limited, 2004

Within Site Networks - 1420




Multimode Optical Fibre Cable




V2.0 © NCC Education Limited, 2004

Within Site Networks - 1421




Monomode Optical Fibre Cable



V2.0 © NCC Education Limited, 2004

Within Site Networks - 1422




Structured Cabling

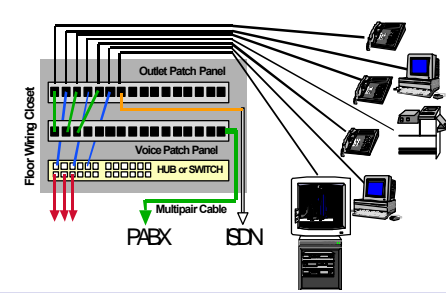
- One cabling scheme for all applications
- Uses category 5, 5e or 6 cable
- Speeds up to 1 Gigabits/s are possible
- Flood wiring of area to be covered
- Standard socket outlets (RJ45)
- Vertical risers often use fibre optic cable
- Strategically located patch panels to facilitate alterations

V2.0 © NCC Education Limited, 2004

Within Site Networks - 1423




Structured Cabling Systems



V2.0 © NCC Education Limited, 2004

Within Site Networks - 1424




Radio

- More flexible than cable
- Easier to install and alter
- Most successful radio-based LANs are based on IEEE 802.11b
- Permits roaming of mobile devices
- Transmission speed is much less than category 5 cabling
- Costs are higher than cable
- Less secure than cable

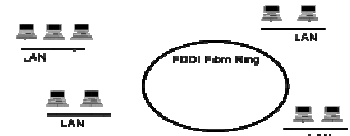
V2.0 © NCC Education Limited, 2004

Within Site Networks - 1425




Fibre Distributed Data Interface (FDDI)

- Uses dual fibre optic cable ring
- 100Mbits/s
- Superseded by 100BaseT Ethernet



V2.0 © NCC Education Limited, 2004

Within Site Networks - 1426




Asynchronous Transfer Mode (ATM)

- Connection orientated
- Cell switching approach
- Fixed size cells (53 Octets)
- Superseded by Gigabit/s Ethernet

V2.0 © NCC Education Limited, 2004

Within Site Networks - 1427




Virtual Network Architecture

Four types in common use:

- Peer-to-peer
- Client/server
- Intranets
- Extranets

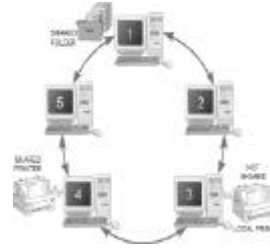
V2.0 © NCC Education Limited, 2004

Within Site Networks - 1428




Peer-to-Peer Networks

- Control of local unit is autonomous
- Resources shared at discretion of individual user
- All nodes can act as both clients and servers




V2.0 © NCC Education Limited, 2004

Within Site Networks - 1429




Client/Server Networks

- LAN control is centralised
- Server holds programs and data for clients
- Server provides security
- Client may not include local hard or floppy drive – known as diskless workstation



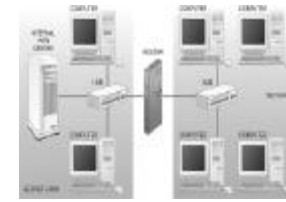
V2.0 © NCC Education Limited, 2004

Within Site Networks - 1430



Intranet

- Private network based on Internet technology
- Owned and managed by a corporation/business
- Access only available to employees
- Built on TCP/IP protocol



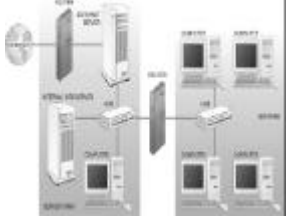
V2.0 © NCC Education Limited, 2004

Within Site Networks – 1431

NCC

Extranet


- Extension of an Intranet
- Also made available to trusted business partners, trading partners etc.
- Enables remote access by mobile employees
- Makes extensive use of firewalls for security



The diagram illustrates an Extranet setup. It shows an internal network (Intranet) on the left, which is connected to an external network (Extranet) on the right. A central firewall device is positioned between the two networks, controlling access. The internal network includes a server and several desktop computers. The external network also includes a server and several desktop computers. A globe icon is shown on the far left, representing the Internet or a wide area network. The diagram is enclosed in a blue border.

V2.0 © NCC Education Limited, 2004

Network Security - 15.1




Enterprise Networking

Session 15
Network Security

V2.1 © NCC Education Limited, 2007

Network Security - 15.2




Objectives

- Understand what is meant by a secure network
- Identify the major threats to network security
- Explain what countermeasures might be used to counteract these threats
- Understand
 - how threats to a network might be analysed in terms of significance to a given organisation/situation and how this would affect the choice of countermeasures used
 - the need for a disaster recovery plan, and the likely components of the plan

V2.1 © NCC Education Limited, 2007

Network Security - 15.3




Secure Network Requirements

The network must offer:

- Privacy
- Integrity
- Availability

V2.1 © NCC Education Limited, 2007

Network Security - 15.4




Privacy

- Reasonable level of assurance that transmitted information
 - is only accessible to authorised users
 - if accessible by non-authorised users, then it is incomprehensible

V2.1 © NCC Education Limited, 2007

Network Security - 15.5




Integrity

- Reasonable level of assurance that transmitted information has not been
 - modified
 - corrupted
 - lost

V2.1 © NCC Education Limited, 2007

Network Security - 15.6



Availability

- Reasonable level of assurance that the network is available for use
 - when needed
 - in the manner needed
 - to provide the functions needed

V2.1 © NCC Education Limited, 2007

Network Security - 15.7




Threats to Security

- Eavesdropping
- Man-in-the-middle interception
- Replay
- Viruses
- Trojan Horses
- Traffic analysis
- Physical attack

V2.1 © NCC Education Limited, 2007

Network Security - 15.8




Eavesdropping

- Involves gaining illicit access to information
- Can be simple as 'borrowing' a computer when the normal user is absent
- Can involved more sophisticated network monitoring
- A significant problem for radio-oriented networks

V2.1 © NCC Education Limited, 2007

Network Security - 15.9




Man-in-the-Middle

- Where a third party pretends to be either party of a two party conversation
- Allows eavesdropping of both sides of conversation
- Presents opportunity to modify information before onward transmission
- Store and Forward message transmission is particularly prone

V2.1 © NCC Education Limited, 2007

Network Security - 15.10




‘Man-in-the-Middle’ Attack

“Can you supply 6,000 widgets by tomorrow afternoon?”

A

“That would be a pleasure! Great to do business with you. By the way, our new company name and address is...”




“I’m sorry - I have an alternative widget supplier now”

B

“That’s a pity perhaps we can do something about our price”

V2.1 © NCC Education Limited, 2007

Network Security - 15.11




Replay

- Allows an attacker to record a sequence of messages for subsequent replaying
- User names or passwords are particularly vulnerable
- Starts as an attack on privacy
- Then becomes an attack on network integrity and then possibly a denial of service

V2.1 © NCC Education Limited, 2007

Network Security - 15.12




Viruses

- Generally of an integrity or service denial nature
- Initially designed to attack users’ computers but very often now designed to attack the network
- Common method is an attachment to emails
- Very often non-malicious (for fun!)

V2.1 © NCC Education Limited, 2007

Network Security - 15.13




Trojan Horses

- **Innocuous program to facilitate illicit access to**
 - networks
 - files
 - stored data
 - steal passwords

V2.1 © NCC Education Limited, 2007

Network Security - 15.14




Traffic Analysis

- **Observation of network usage can often provide other information such as**
 - identifying associations
 - business dealings
 - customers

V2.1 © NCC Education Limited, 2007

Network Security - 15.15




Physical Attack

- **Can be deliberate or accidental**
- **Usually results in a denial of service**
- **Accidental is usually due to**
 - fire
 - lighting
 - flood
 - earthquake
 - equipment failure
- **Deliberate often due to**
 - fire
 - theft
 - malicious damage

V2.1 © NCC Education Limited, 2007

Network Security - 15.16




Denial of Service (DoS) Attacks

- **Assault on a network, flooding it with requests**
- **May also use ‘mailbombing’**
- **Result is that network service is either slowed or completely interrupted for some time**
- **Can also use multiple computers throughout network for Distributed Denial of Service attack**
- **Typically results in serious loss to the organisation affected – either in time or money**

V2.1 © NCC Education Limited, 2007

Network Security - 15.17




Minimising DoS Attacks

- **Install route filters**
- **Install patches to guard against TCP SYN flooding**
- **Disable all unused network services**
- **Enable quota systems on operating system**
- **Observe system performance**
- **Invest in and maintain ‘hot spares’**
- **Invest in redundant/fault tolerant network configurations**
- **Maintain password policies**

V2.1 © NCC Education Limited, 2007

Network Security - 15.18




Phishing

- **Becoming a major threat for Internet users**
- **Email sent to user claiming to be from a legitimate enterprise**
- **Intended to fool user into divulging personal information such as bank account details, passwords, PIN numbers etc**
- **Once information has been obtained, it is used to fraudulently obtain money or purchase goods**

V2.1 © NCC Education Limited, 2007

Network Security - 15.19




Countermeasures

- Authentication
- Encryption
- Digital signatures
- Virus detection and/or protection
- Firewalls
- Physical

V2.1 © NCC Education Limited, 2007

Network Security - 15.20




Authentication



- User name and associated password
- Known personal information
- Personal Identification Numbers (PINs)
- Recognition
 - fingerprint
 - voice
 - handwriting
- Smart cards
- DNA matching
- Retinal scans

V2.1 © NCC Education Limited, 2007

Network Security - 15.21



Example of Authentication

“Who goes there?” →

← “Arthur”


“What’s the password?” →

← “Camelot”

“Sorry you’re not allowed in here!” →

V2.1 © NCC Education Limited, 2007

Network Security - 15.22




Encryption

- Changing original information into a form only recognisable to the sender and receiver
- Sender and receiver need to know the ‘key’ to be able to code and decode the information
- Usually involves a complex and time consuming mathematical process
- Key distribution is often a problem as it allows the key to be stolen
- ‘Public key encryption’ solves key distribution problem

V2.1 © NCC Education Limited, 2007

Network Security - 15.23




Digital Signatures

- A means of proving that the sender of a document is genuine
- A means of indicating that a document has not been modified
- Sender creates a mathematical summary of a document
- Sender uses a private key to encrypt the summary
- Recipient calculates the summary using the same function as the sender
- Recipient uses the sender’s public key to decode signature
- If recipient’s calculated summary matches the extracted summary by decoding the signature then the document will be genuine
- Closely related to ‘certificates’

V2.1 © NCC Education Limited, 2007

Network Security - 15.24




Virus Protection

- Virus detection and protection programs are only effective if regularly updated
- Network access software also needs regular updating
- User education to detect non-trusted sources of information is also of prime importance

V2.1 © NCC Education Limited, 2007

Network Security - 15.25




Firewalls (1)

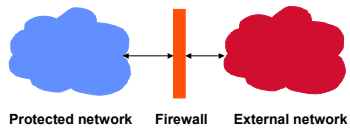
- Devices to police traffic that enters and leaves a given area of a network
- Positioned so that external traffic must pass through the firewall
- Can protect the network by:
 - preventing unauthorised network access
 - selectively permitting access to defined areas
 - selectively filtering of incoming email messages
 - performing virus checking of email file attachments
 - preventing staff from accessing non work-related web sites
 - preventing users from performing file transfers into a protected network

V2.1 © NCC Education Limited, 2007

Network Security - 15.26




Firewalls (2)



Protected network Firewall External network

V2.1 © NCC Education Limited, 2007

Network Security - 15.27




Virtual Private Networks (VPNs)

- Enable businesses to use Internet backbone for private data communications
- Uses encryption and encapsulation technologies
- Carves out a private passageway on the Internet
- Frequently used by remote offices and mobile workers
- Provides substantial savings on cost of private network bandwidth

V2.1 © NCC Education Limited, 2007

Network Security - 15.28




Secure IP (IPSEC)

- Protocol suite designed to provide a standard way for protecting all Internet traffic
- Will work irrespective of application
- Uses modern cryptographic methods to protect against eavesdropping and modification
- Supports two encryption modes
 - Transport mode
 - Tunnel mode

V2.1 © NCC Education Limited, 2007

Network Security - 15.29




Point to Point Tunnelling Protocol (PPTP)

- Enhanced version of PPP
- Developed by US Robotics
- Implemented at both ends of a point to point connection across the Internet
- Encapsulates the data and encrypts it prior to transmission
- Can be used to construct a VPN

V2.1 © NCC Education Limited, 2007

Network Security - 15.30




Physical Countermeasures

- Fire prevention and detection
- Securing wiring and equipment accommodation areas
- Preventing unauthorised access to accommodation

V2.1 © NCC Education Limited, 2007

Network Security - 15.31




Choice of Countermeasures

- Although possible to prevent all breaches in security this is rarely economic
- Necessary to assess the implication of a breach to ascertain the value of prevention
- Need to appreciate that a network cannot be rendered completely secure and very often attempts to do so will be counterproductive

V2.1 © NCC Education Limited, 2007

Network Security - 15.32




Business Continuity

- Provision of off-site data centres to mirror business critical information
- Availability of alternative office accommodation
- Provision of temporary telephone service
- Provision of replacement office facilities (desks etc.)
- Hiring of temporary staff

V2.1 © NCC Education Limited, 2007

Networking Planning - 16.1




Enterprise Networking

Session 16
Networking Planning

V2.0 © NCC Education Limited, 2004

Networking Planning - 16.2




Objectives

- Appreciate the importance of traffic analysis to network design and the role played by the queuing theory
- Understand the
 - arguments involved in choosing appropriate bearers
 - decisions made to choose the technology to be adopted
- Appreciate the reasons for ensuring network resilience

V2.0 © NCC Education Limited, 2004

Networking Planning - 16.3




Network Planning Factors

- Capacity requirements – traffic analysis
- Choice of bearers – related to capacity needs
- Choice of technology – interacts with both of the above
- Network security – increasingly vulnerable to threats
- Implementation – how, when and where work is undertaken

V2.0 © NCC Education Limited, 2004

Networking Planning - 16.4




Traffic Analysis

- Factors affecting logical information flows:
 - traffic volumes
 - traffic types
 - costs
 - physical considerations
 - technological considerations
- Given the types of information and the number of messages flowing between two nodes it is possible to calculate the aggregate traffic
- Aggregate traffic can indicate minimum data transmission rate

V2.0 © NCC Education Limited, 2004

Networking Planning - 16.5




Timing Considerations

- Need to assess how long it takes to transmit a message
- Time to transmit will affect capacity (bandwidth)
- Type of traffic will influence transmission time demands

V2.0 © NCC Education Limited, 2004

Networking Planning - 16.6




Cost and Resilience

- One affects the other
- Rarely practical or cost-effective to have dedicated links between all nodes
- Some degree of redundancy is important:
 - importance of traffic
 - impact on business
 - time to repair
 - physical threats
 - physical alternative routing
 - load sharing possibilities

V2.0 © NCC Education Limited, 2004

Networking Planning - 16.7




Queuing Theory

- Networks may have ability to queue messages
- Queue length is important
- Queue lengths affect flow control
- Queuing theory presents a mathematical basis for calculating queue lengths:
 - takes no account of flow control techniques
 - theory is complex for reasonable size networks
 - more practical to use simulation

V2.0 © NCC Education Limited, 2004

Networking Planning - 16.8




Network Simulation

Should include the following features:

- Traffic analysis
- Identification of bottlenecks
- Resilience against failure
- Available accommodation
- Network costing

V2.0 © NCC Education Limited, 2004

Networking Planning - 16.9




Choice of Bearers

- Available types are:
 - twisted copper pair cable
 - coaxial cable
 - fibre optic cable
 - radio transmission
- Factors affecting choice:
 - terrain to be covered
 - economics
 - resilience against failure
 - types of service needed

V2.0 © NCC Education Limited, 2004

Networking Planning - 16.10




Choice of Technology

- Historically the technology available at the time was a major influencing factor
- Nowadays digital technology has gained universal acceptance

V2.0 © NCC Education Limited, 2004

Networking Planning - 16.11




Data Rate Requirements

- Analysis of logical information flows is likely to indicate required data rates
- Other factors to be taken into consideration include
 - available rates
 - full or half duplex operation
 - traffic segregation
 - future expansion

V2.0 © NCC Education Limited, 2004

Networking Planning - 16.12




Available Data Rates

- Optical transmission is removing data rate limitations
- Access to the wide area network still has limitations
- Many large businesses have optical access
- Residential and Small Business retain limitations

V2.0 © NCC Education Limited, 2004

Networking Planning - 16.13




Future Network Expansion

- Future capacity needs to be taken into account
- Optical technology development is keeping pace with capacity demands
- Where optical technology cannot be used a problem may result

V2.0 © NCC Education Limited, 2004

Networking Planning - 16.14




Network Resilience

- Traffic analysis requirements will indicate need for resilience
- Reduction in cost of optical technology is making resilience much easier
- Automatic alternative routing capability of SPC exchanges is very helpful
- Network failure, although unavoidable, can be hidden from users

V2.0 © NCC Education Limited, 2004

Networking Planning - 16.15




Security Considerations

- Users are placing considerably more reliance on networks
- Threats to security include loss of:
 - availability
 - integrity
 - confidentiality

V2.0 © NCC Education Limited, 2004

Networking Planning - 16.16




Loss of Availability

Network failures can be caused by:

- Line failure
- Equipment failure
- Power supply failure
- Natural disasters (fire, flood etc.)
- Malicious damage

V2.0 © NCC Education Limited, 2004

Networking Planning - 16.17




Loss of Integrity

- Data is either corrupted or missing
- Largest single source of loss of integrity is viruses
- Firewalls and improved security is helpful

V2.0 © NCC Education Limited, 2004

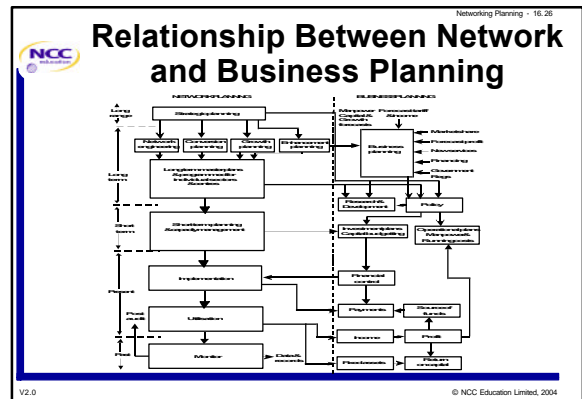
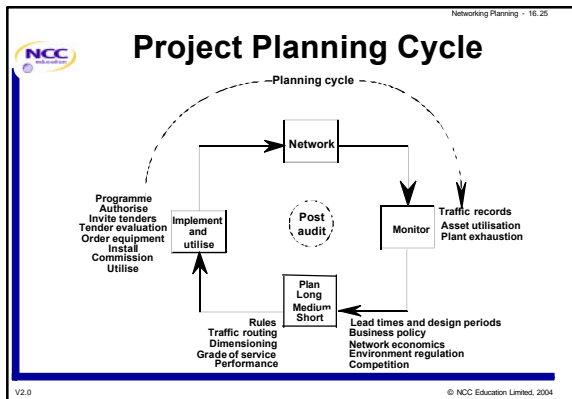
Networking Planning - 16.18



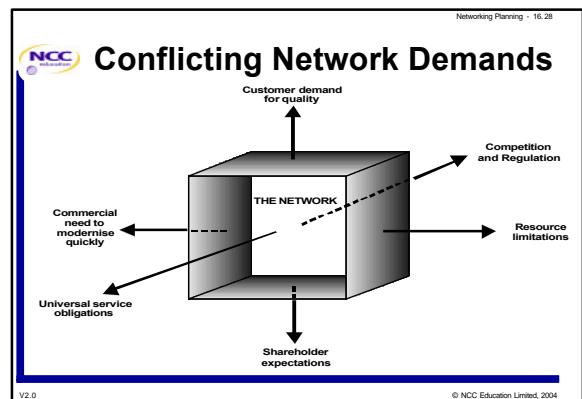
Loss of Confidentiality

- Commonly know as ‘hacking’
- Unauthorised individuals gaining access to information
- Can be reduced by applying right controls and procedures
- Data encryption is also useful

V2.0 © NCC Education Limited, 2004




- ### Strategic Planning
- Individual component networks must fit and co-exist
 - The future of the network should be charted over a 10 to 20 year time frame
 - Future plans are needed for
 - technology
 - architecture
 - management systems
 - performance
 - customer equipment
 - network standards
 - business organisation
 - skills needed for operation and support
- © NCC Education Limited, 2004



- ### Migration Planning
- An existing network may need to be augmented or superseded
 - Plans should ensure existing systems are not disrupted
 - Radical changes are often unavoidable
- © NCC Education Limited, 2004

- ### Network Engineering
- Planning a network to support specific new services or products
 - Commences with product or service definition
 - features required by users
 - forecast of usage in terms of connections and traffic
 - Compliance with international standards
 - Subject to normal planning processes
- © NCC Education Limited, 2004

Networking Planning - 16.31




Growth Planning

- Long term estimates are unlikely to be accurate
- Estimates must be undertaken to ensure planned facilities are capable of meeting long as well as short term growth
- Need to identify new site requirements
- May well trigger a need to develop subsidiary systems

V2.0 © NCC Education Limited, 2004

Networking Planning - 16.32




Enhancement Planning

- Identify the possibility of
 - reducing costs
 - improving performance
 - increasing flexibility
- May identify fault prone areas which, if re-designed, could materially affect the performance of the entire network

V2.0 © NCC Education Limited, 2004

Networking Planning - 16.33




Long Term Planning

- Strategic and implementation plans do not take account of specific needs
- Specific needs will need continuous updating

V2.0 © NCC Education Limited, 2004

Networking Planning - 16.34




Short Term Planning

- Continuous review of
 - growth
 - migration implementation
 - enhancement implementation
 - introduction of new services

V2.0 © NCC Education Limited, 2004

Networking Planning - 16.35




Post Implementation Audit

- Will produce numerous benefits
- Will do more than simply indicate if forecasts were accurate

V2.0 © NCC Education Limited, 2004

Networking Planning - 16.36




Budgeting

- End product of planning process is expenditure
- Unless expenditure is carefully controlled the financial viability of a project may be jeopardised
- Can be avoided by establishing a budget to
 - track all items of project expenditure
 - highlight expenditure overrun
 - ideally prevent expenditure overrun

V2.0 © NCC Education Limited, 2004

Networking Planning - 16.37




Planning Standards

- **Telecommunications networks must be seamless when interfacing with other networks**
- **Only way to achieve this is through the adoption of established standards**
- **Overall network plans must fit comfortably with plans for**
 - numbering
 - charging
 - performance
 - routing
 - signalling
 - switching

V2.0 © NCC Education Limited, 2004

Networking Planning - 16.38




Other Planning Parameters

- **Design periods**
- **Planning lead times**
- **Topology**

V2.0 © NCC Education Limited, 2004

Networking Planning - 16.39




Design Periods

- **Customary to provide networks in stages**
- **Entails careful prediction of demands without involving expansion**
- **Often difficult because of advantages of bulk purchase of equipment**
- **Frequent augmentation increases likelihood of disruption**
- **Typical design periods:**
 - sites – 20 to 40 years
 - buildings – 10 to 20 years
 - switching and transmission plant – 2 to 3 years
 - cables – 5 to 10 years
 - ducting – 20 years

V2.0 © NCC Education Limited, 2004

Networking Planning - 16.40




Planning Lead Times

- **Standard periods allocated to**
 - planning
 - procurement
 - installation
- **Set to make provision for all major events**
- **Allows all activities to fit together to achieve the agreed 'bring-into-service' date**

V2.0 © NCC Education Limited, 2004

Networking Planning - 16.41




Forecasting

- **Size of today's networks means there is significant delay between planning and implementing**
- **Longer planning timescale means less accurate forecasting**
- **Rolling forecasts are therefore used**
- **An entirely new service will not have the benefit of past experience**
- **Characteristics of a new service may be totally different from any existing service**
- **Competition also introduces another factor**

V2.0 © NCC Education Limited, 2004

Networking Planning - 16.42



Network Optimisation

- **Current demands are such that all networks must operate at peak efficiency**
- **Constitutes a need for network optimisation**
- **Entails studies of switching and transmission plant in conjunction with traffic routing to achieve optimum solution**
- **Lowest cost option to meet minimum standard for a given demand**
- **Alternatively maximising quality for a given demand or cost, or maximising capacity of a given demand**

V2.0 © NCC Education Limited, 2004

