MODULE 1: INTRODUCTION TO NETWORKS

NETWORK+ 007

Your fastest way to learn. Guaranteed.

FIREBRAND

WHAT IS A NETWORK

"Two or more connected computers that can share resources such as data and applications"

Determined by:

- Type of Computer
- Topology
- Interconnection device

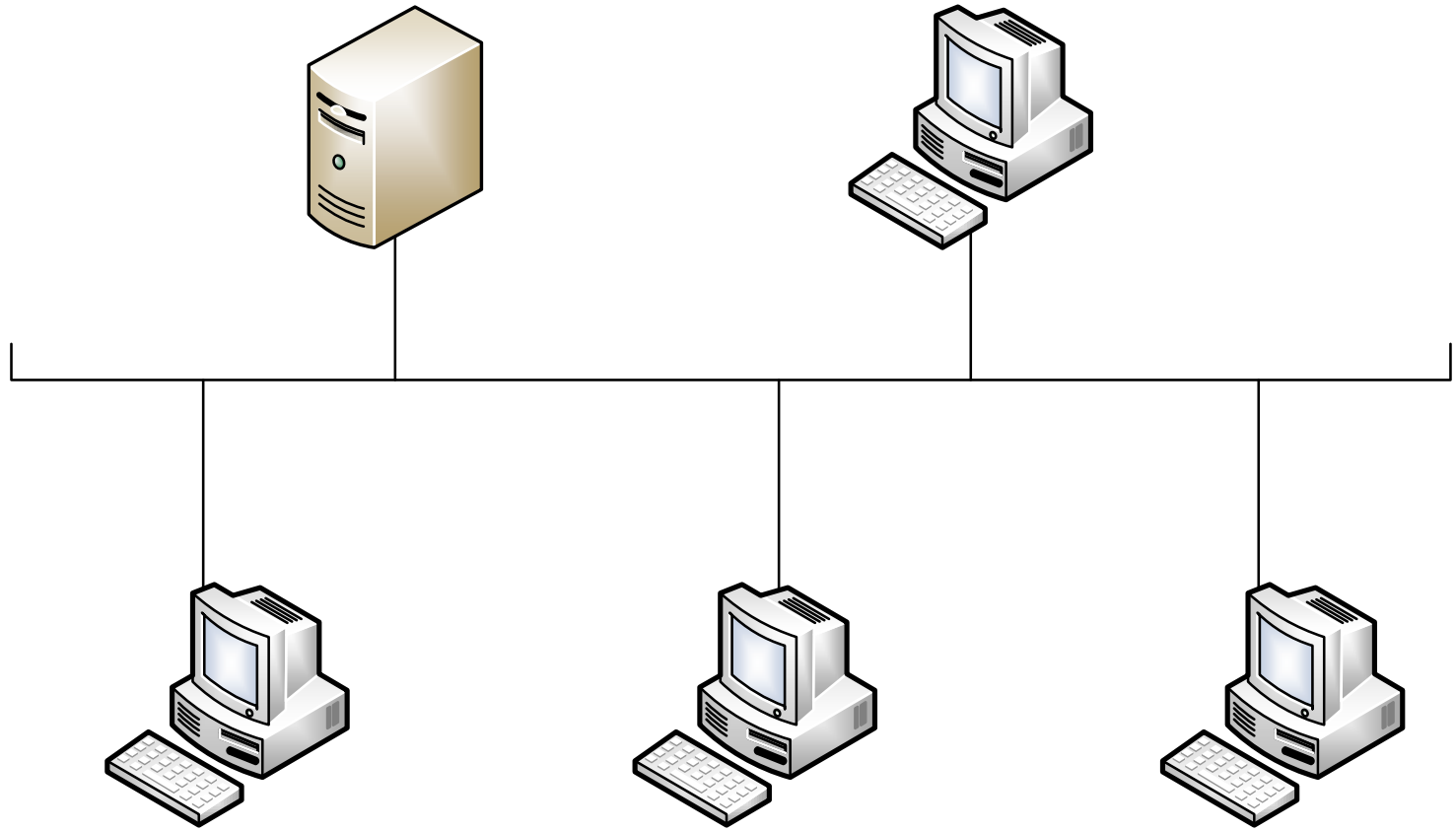
CLIENTS AND SERVERS

Types of Computer

- Workstation / Client
- Server
- Types of Network
- Peer-Peer
- Client-Server

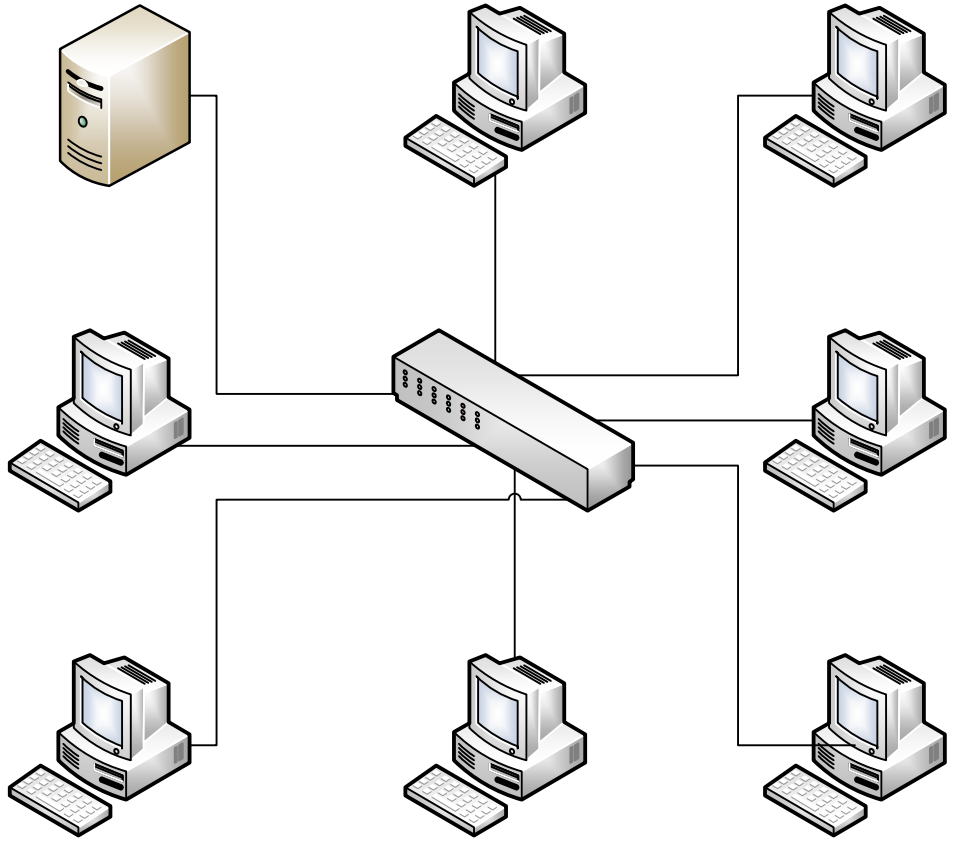
NETWORKING TOPOLOGY

BUS



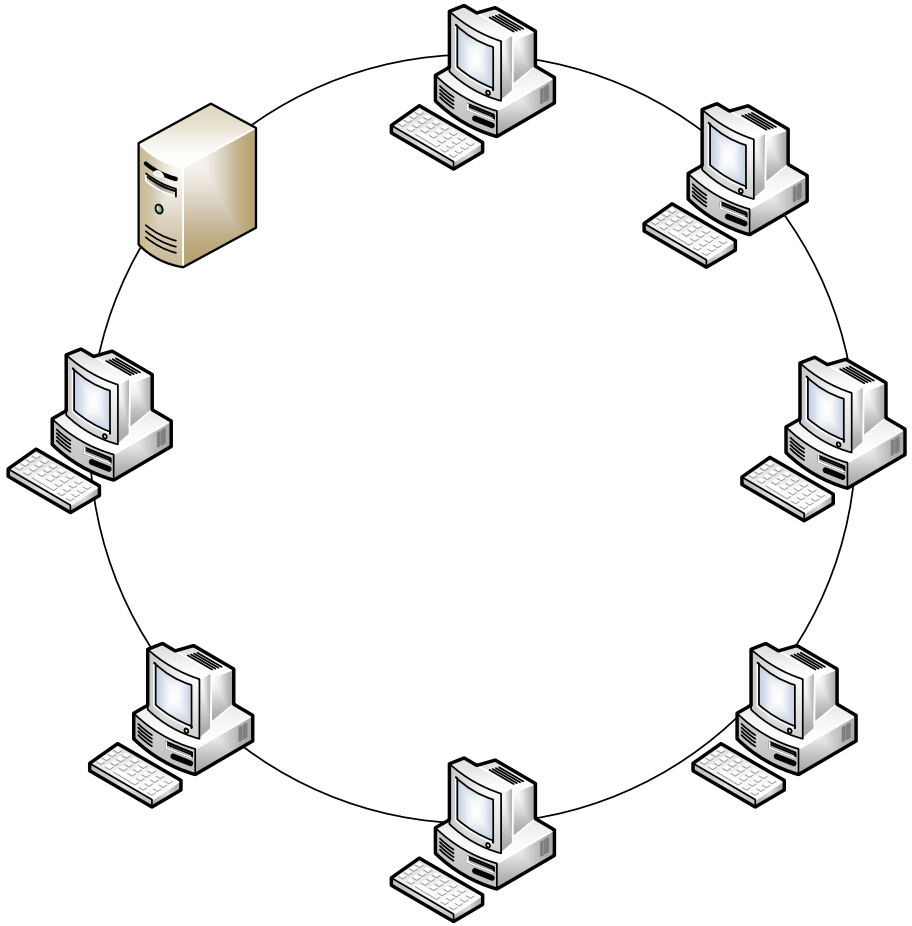
NETWORKING TOPOLOGY

Star (Hub and Spoke)



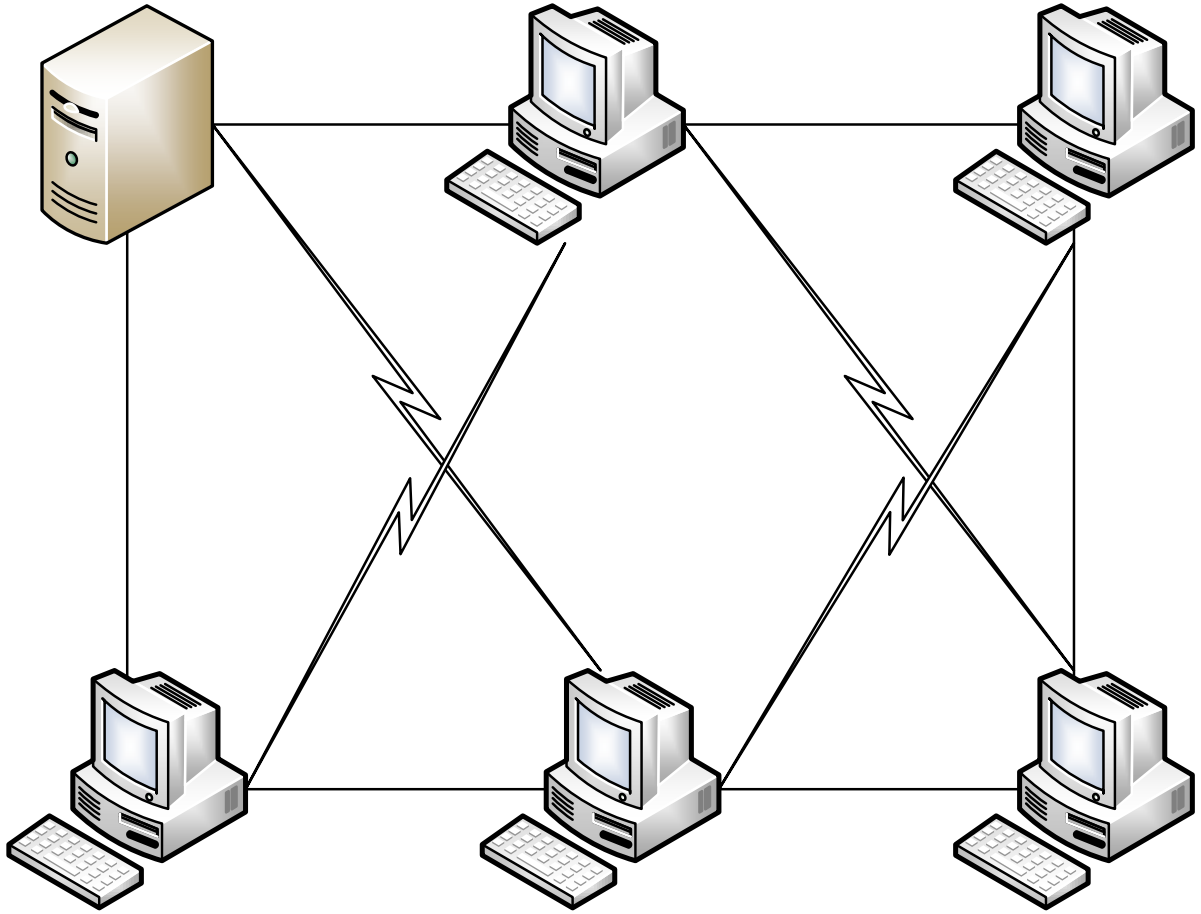
NETWORKING TOPOLOGY

RING



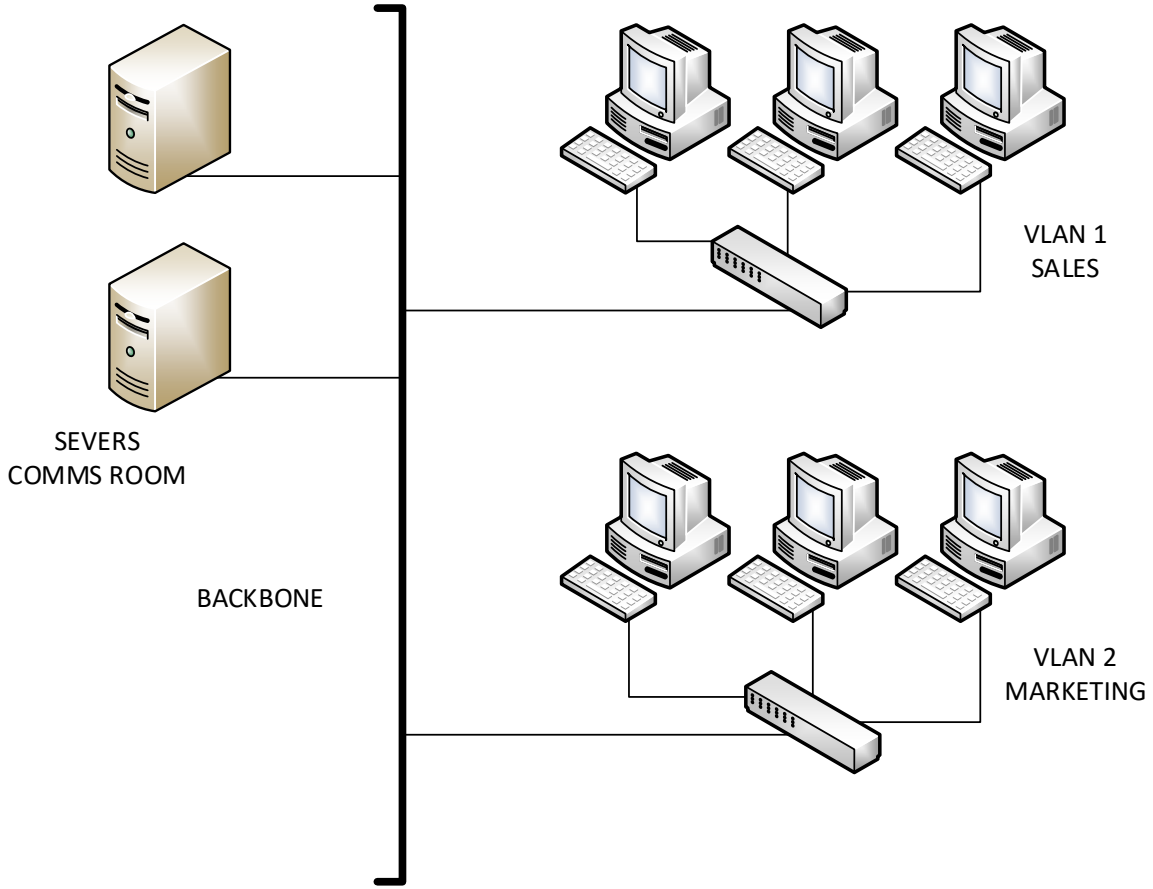
NETWORKING TOPOLGY

MESH



NETWORKING TOPOLOGY

Backbone and Segments



NETWORK TYPES

LAN – Local Area Network
MAN – Metropolitan Area Network
WAN – Wide Area Network
PAN – Personal Area Network

RACK MOUNT SERVERS

These are servers designed to be bolted into a framework called a rack and thus are designed to fit one of several standard size rack slots, or bays. They also require rail kits, which when implemented allow you to slide the server out of the rack for maintenance.

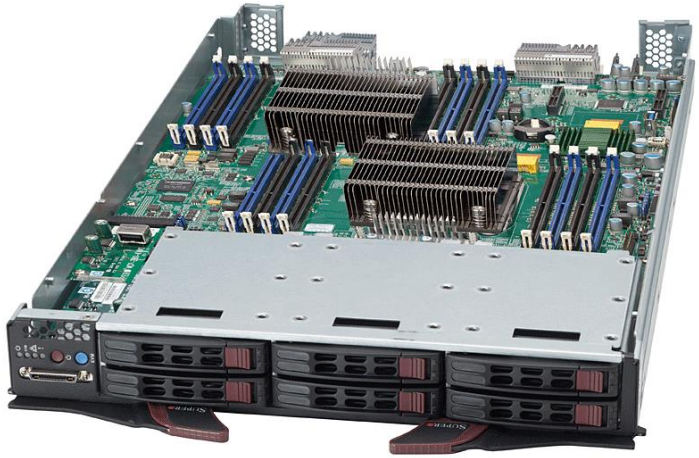
One of the benefits of using racks to hold servers, routers, switches, is that a rack gets the equipment off the floor, while also making more efficient use of the space in the server room and maintaining good air circulation. Measure in U where 1U = 1.75 inches high.

TOWER SERVERS

A Tower server bears the most resemblance to the workstations you are used to working with. When many of these devices are used in a server room, they reside not in the rack but on shelves.

BLADE SERVERS

Consists of a server chassis housing multiple thin, modular circuit boards, known as server blades. Each blade (or card) contains processors, memory, integrated network controllers, and other input/output (I/O) ports. Servers can experience as much as an 85 percent reduction in cabling for blade installations over conventional 1U or tower servers. Blade technology also uses much less space



MODULE 2:THE OSI REFERENCE MODEL

NETWORK+ 007

Your fastest way to learn. Guaranteed.

FIREBRAND

THE OPEN SYSTEMS INTERCONNECTION MODEL

The OSI model is the primary architectural model for networks.

- It describes how data and network information are communicated from an application on one computer through the network media to an application on another computer.
- The OSI reference model breaks this approach into 7 layers.

"*All People Seem To Need Data Processing*"

OSI REFERENCE MODEL

7 APPLICATION

The application layer provides connectivity between users and application processes to access network services. This layer contains a variety of commonly needed functions:

- Resource sharing *NFS FTP HTTP*
- Network management *SNMP TELNET*
- Directory services *LDAP*
- Electronic messaging (such as mail) *SMTP, POP3*

6 PRESENTATION

The presentation layer formats the data to be presented to the application layer. It acts as the 'translator' for the network.

The presentation layer provides:

- Character code translation.
- Data conversion.
- Data compression: reduces the number of bits that need to be transmitted on the network.
- Data encryption: encrypt data for security purposes. For example, password encryption.

5 SESSION

The session layer allows session establishment between processes running on different stations. It provides:

- Session Management – establishment and termination between two application processes on different machines
- Session support allowing processes to communicate over the network, performing security, name recognition, logging, and so on.

4 TRANSPORT

The transport layer ensures that messages are delivered error-free, in sequence, and with no losses or duplications.

The transport layer provides:

- Message segmentation
- Message acknowledgment
- Message traffic control
- Session multiplexing
- **Transmission Control Protocol (TCP) / User Datagram Protocol (UDP) both work at Layer 4**

3 NETWORK

The network layer controls the operation of the subnet, deciding which physical path the data should take based on network conditions, priority of service, and other factors. It provides:

- Routing
- Subnet traffic control through the use of a router (Layer 3 Intermediate system)
- Frame fragmentation
- Logical-physical address mapping
- **Internet Protocol (IPv4 / IPv6)**

2 DATALINK

The data link layer provides error-free transfer of data frames from one node to another over the physical layer. The data link layer provides:

- Link establishment and termination
- Frame traffic control
- Frame sequencing
- Frame acknowledgment
- Frame error checking
- Media access management

OSI – DATALINK LAYER

The IEEE Ethernet Data Link layer has two sublayers
Media Access Control (MAC)
Logical Link Control (LLC)

Devices which work at Layer 2 include:

- Switch
- Network Adaptor
- Bridge

OSI – DATALINK LAYER – IEEE 802 STANDARDS

IEEE 802. STANDARD	Topic
802.1	LAN/MAN Management
802.2	Logical Link Control
802.3	**CSMA/CD ETHERNET**
802.8	Fiber-Optic LAN/MAN
802.10	LAN/MAN Security
802.11	**Wireless LAN**

1 PHYSICAL

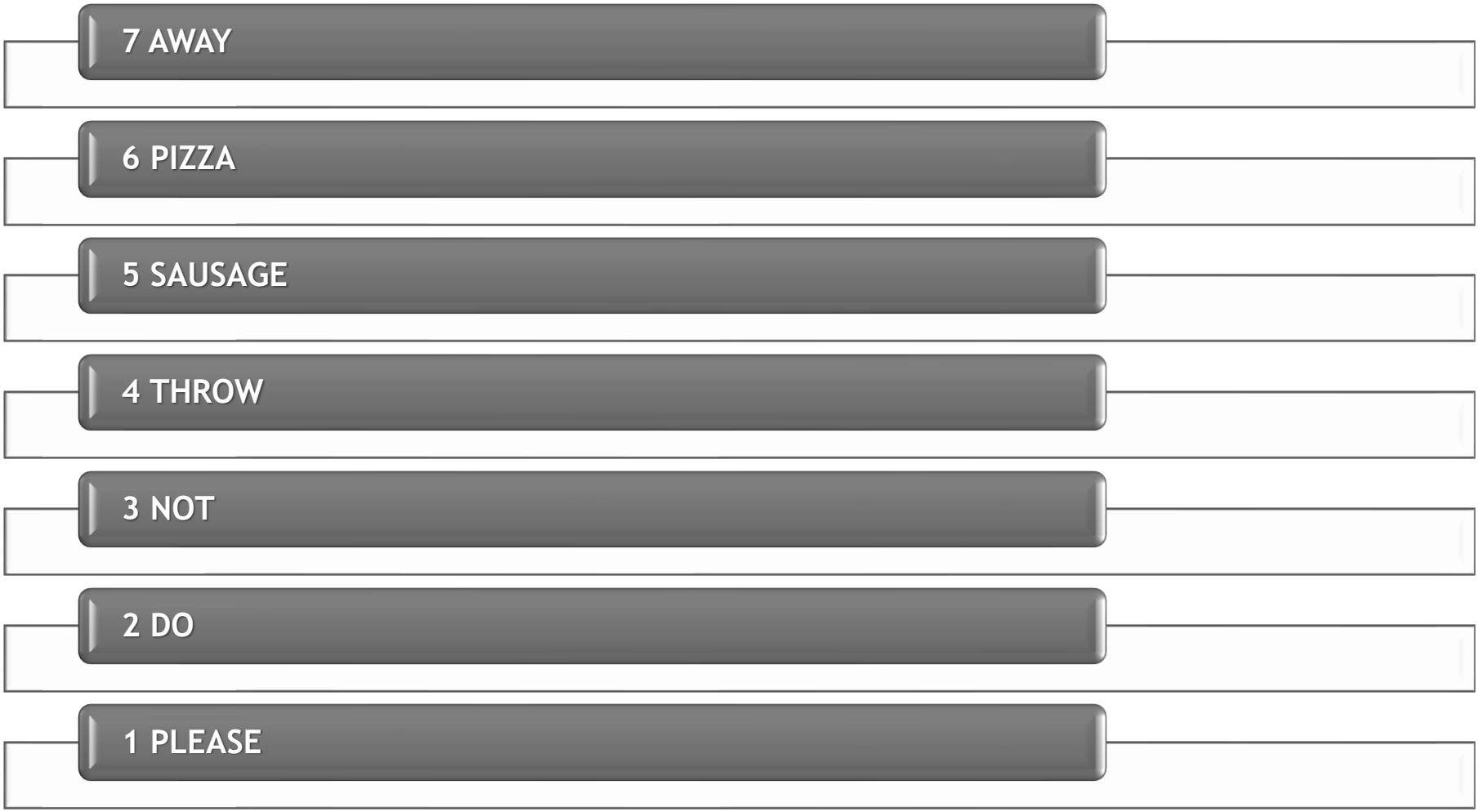
The physical layer is concerned with the transmission and reception of the unstructured raw bit stream over a physical medium. It provides:

- Data encoding
- Physical medium attachment
- Physical medium transmission

Devices that work at Layer 1 include:

- Hub
- Repeater
- Media Convertor

PLEASE DO NOT THROW SAUSAGE PIZZA AWAY!



MODULE 3: NETWORKING TOPOLOGY, CONNECTIONS AND WIRING STANDARDS

NETWORK+ 007

Your fastest way to learn. Guaranteed.

FIREBRAND

CABLE CHARACTERISTICS

- Cost
- Installation issues
- PLENUM Rating
- Bandwidth/Speed/Capacity
- Duplex/Half Duplex
- Serial/Parallel
- Distance/Attenuation
- Noise immunity
- Security

TYPES OF COXIAL CABLE

Network Type	Coax Type	Max Distance
Thin Ethernet baseband	RG58	185 METRES
Thick Ethernet baseband	RG8 / RG11	500 METRES
Cable TV broadband	RG6	Variable

TYPES OF CABLE

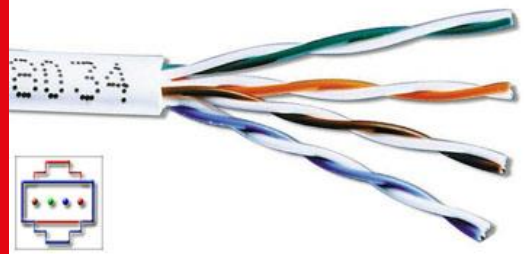
- Coax connectors
- BNC
- F

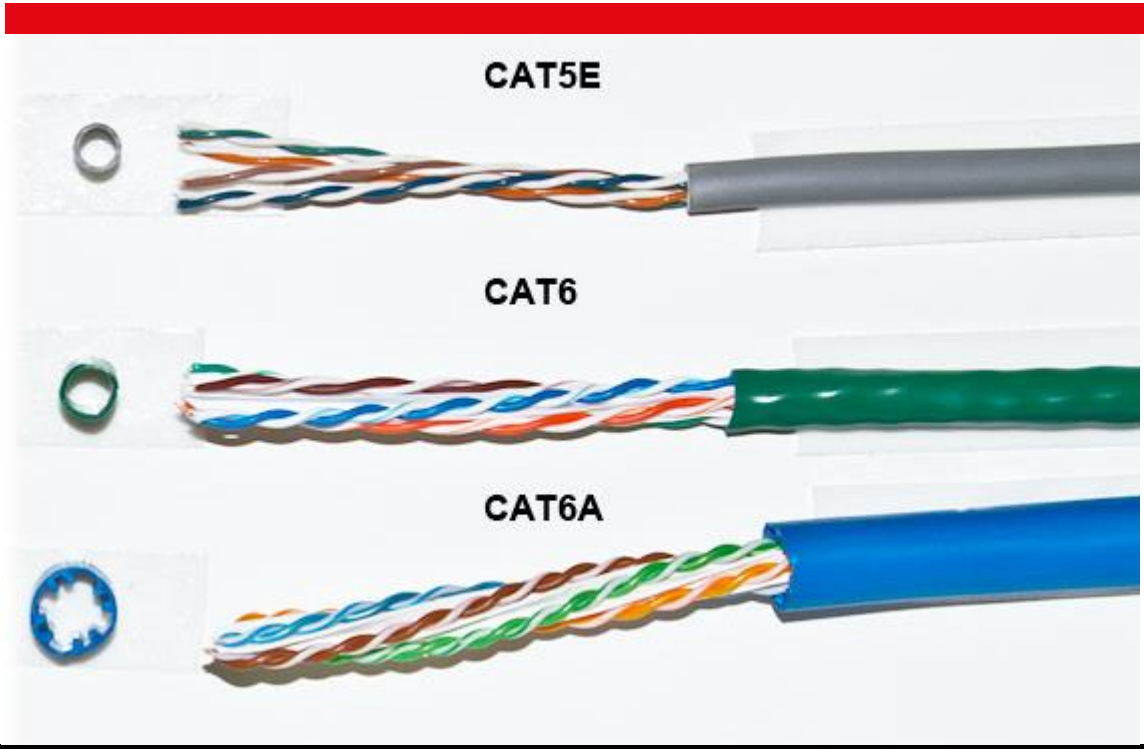
TYPES OF CABLE

- Twisted Pair
- UTP
- STP
- CAT standards
- Connectors

Shielded twisted pair (STP)

Unshielded twisted pair (UTP)





CAT TYPES

Cat 5e Four twisted pairs rated for 100 MHz, but can handle all four pairs transmitting at the same time (required for GB Ethernet). Cat 5 is essentially redundant (can you still buy it??).

Cat 6 Four twisted pairs rated for 250 Mhz. A standard from 2002. Used as a riser cable to connect floors, but for future proof best practice to install as standard for a new network.

RJ45

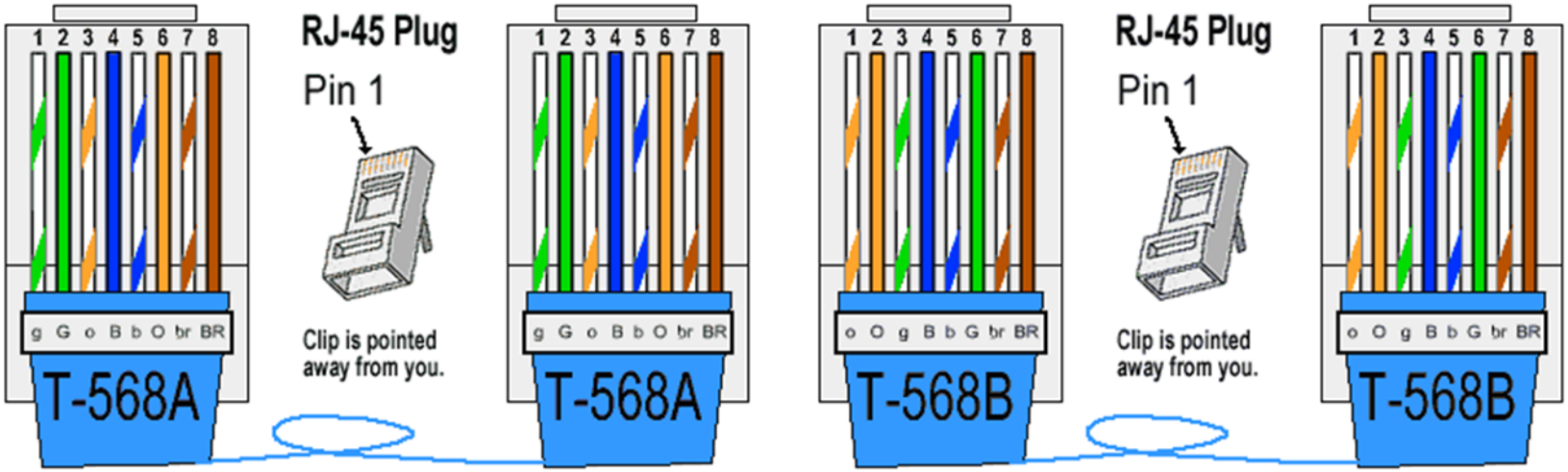
- RJ45 plugs and sockets are most commonly used as connectors for Ethernet cable (UTP)
- Also known as 8P8C (8 position 8 Contact)
- Eight equally spaced conductors
- Terminated using a crimp tool

RJ45 WIRING STANDARDS

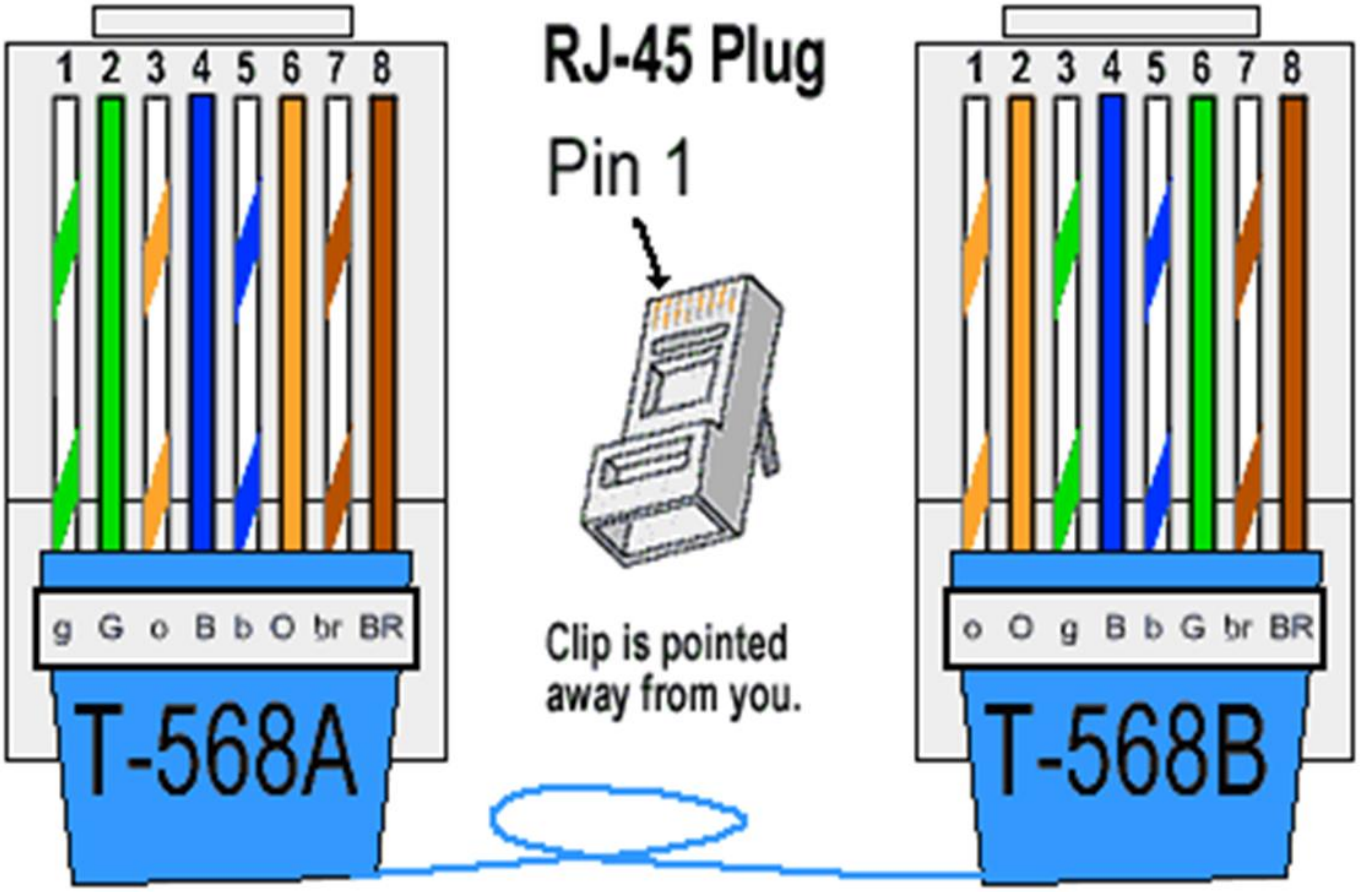
- T568A
- T568B
- STRAIGHT THROUGH
- CROSSOVER
- ROLLOVER
- LOOPBACK

T568A / T568B

T568B is more common

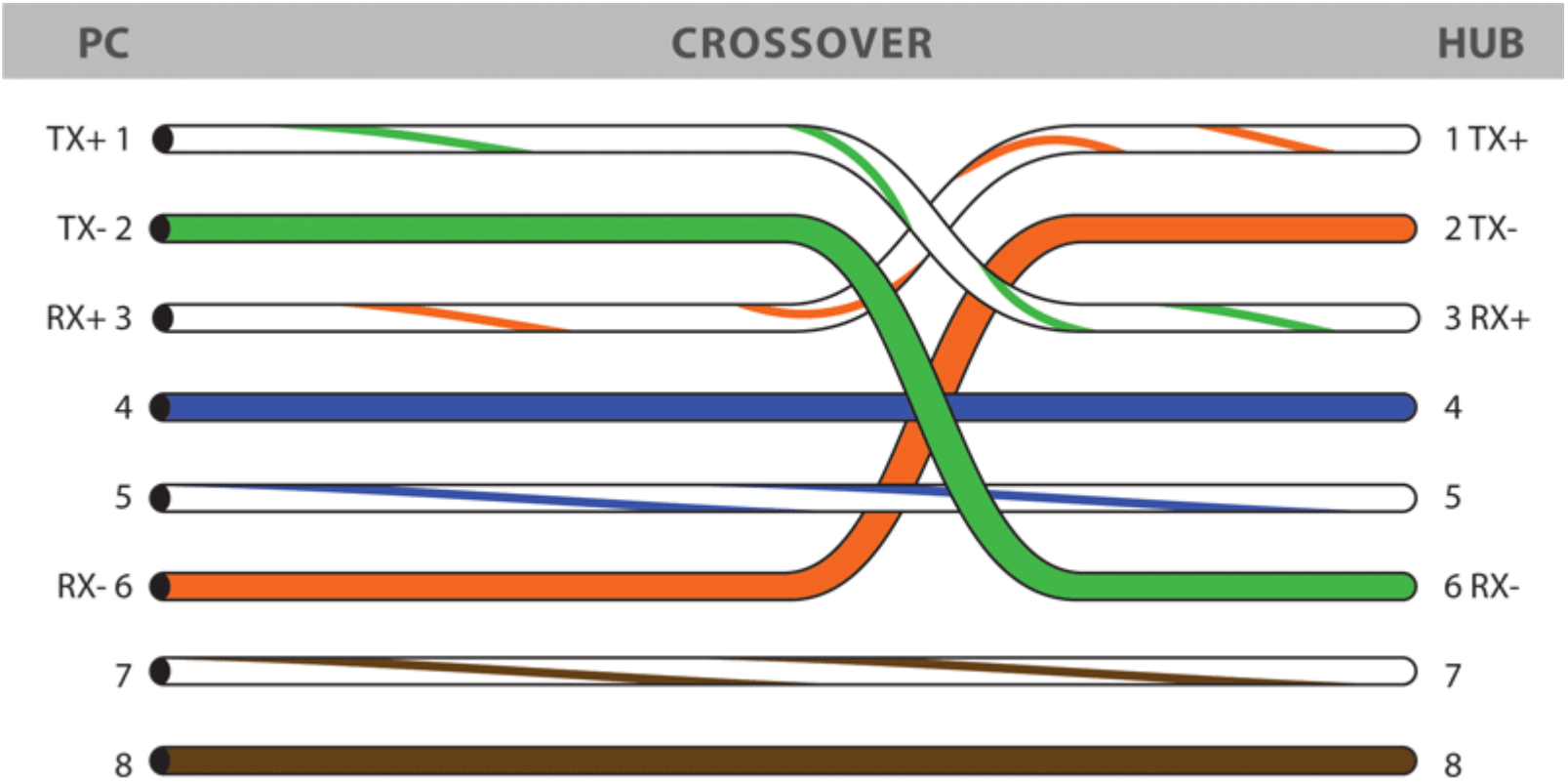


CROSSOVER



LAB

Create your own crossover cable



ROLLOVER AND LOOPBACK CABLE

Console Cable used to connect Administrator to console port of a Router or Switch

Loopback Cable used for diagnostics and testing.

FIBER OPTIC

- ST Connector (Straight Tip)
- SC Connector (Subscriber Connector)
- LC Connector (Local Connector)
- MTRJ (Mechanical Transfer Registered Jack)
- Single Mode Fibre (SMF)
- Multimode Fibre (MMF)

MEDIA CONVERTER

Allow the conversions between different types of Fibre Optic or between Fibre and Ethernet.

These include:

- Single Mode Fibre to Ethernet
- Multi Mode Fibre to Ethernet
- Fibre to Coaxial

TYPES OF CABLE

Other types of communications cables include:

- RS232
- USB
- FIREWIRE
- THUNDERBOLT

PATCHING AND CABLING

MDF – Main Distribution Frame is a terminating point where cables are connected and can be jumpered to different locations

IDF – Intermediate Distribution Frame, a smaller version of the MDF maybe on each floor of a building

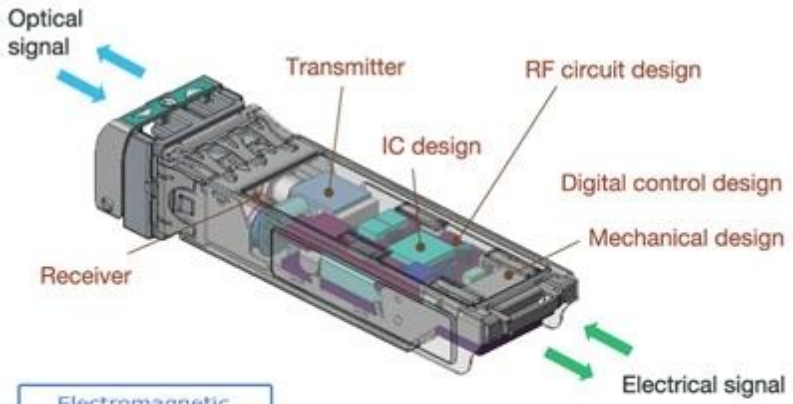
Patch Panel – where circuits can be rerouted through the use of CAT 5 patch leads

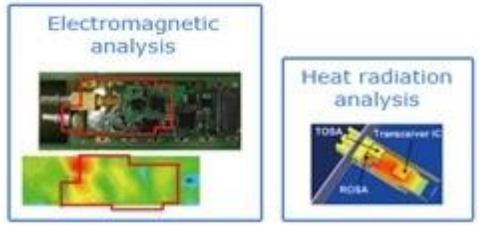
66 / 110 BLOCK

66 Block used for Telephone systems
110 Block used for Cat 5/6 UTP systems
Fibre distribution panel

TRANSCEIVER

Transceiver is a transmitter and a receiver, a device that both transmits and receives analogue or digital signals. The term is used most frequently to describe the component in local-area networks (LANs) that applies signals onto the network wire and detects signals passing through the wire.





DEMARCATION POINT

The **DEMARC** or demarcation point is the point at which the telephone company or circuit provider network ends and connects to the wiring at the customer's premises.

A box such as an NIU (Network Interface Unit) or a CSU (Channel Service Unit) which carries out code or protocol conversion is commonly referred to as a **SMART JACK.** This is the terminating point between the TELCO and the customer network

MODULE 4:ETHERNET SPECIFICATIONS

SECURITY+ 007

Your fastest way to learn. Guaranteed.

FIREBRAND

INTRODUCTION TO ETHERNET

The MAC address Ethernet Media Access Control address – the “physical” address of a network adapter

- Unique to a device 48 bits / 6 bytes long and displayed in hexadecimal
- Half-duplex - a device cannot send and receive simultaneously
- All LAN hubs are half-duplex devices
- Full-duplex - data can be sent and received at the same time
- A properly configured switch interface will be set to full-duplex

CARRIER SENSE MULTIPLE ACCESS / COLLISION DETECTION CSMA/CD

Short for Carrier Sense Multiple Access / Collision Detection.

- A set of rules determining how network devices respond when two devices attempt to use a data channel simultaneously (called a collision).
- Standard Ethernet networks use CSMA/CD to monitor the traffic on the line at participating stations.
- No transmission means the particular station can transmit.
- If two stations try to communicate at the same time this would cause a collision

CSMA/CA (COLLISION AVOIDANCE)

- Used on Wireless Networks
- Nodes have to listen to detect if network is busy before sending
- Optionally may be implemented with Request To Send/Clear To Send (RTS/CTS)

ETHERNET STANDARDS 802.3

Ethernet descriptive labels

Eg: **10Base5**

Equates to:

10 Mbps

Baseband signalling (one channel of communication at any time)

500 Metres maximum length

10Base2 (runs for 185 Metres)

COMMON ETHERNET CABLE TYPES

Ethernet Name	Cable Type	Max Distance	Notes
10Base5	COAX	500m	Thicknet
10Base2	COAX	185m	Thinnet
10BaseT	UTP	100m	
100BaseTX	UTP/STP	100m	Cat5 upwards
10BaseFL	FIBER	500-2000m	Ethernet over Fiber
100BaseFX	MMF	2000m	
1000BaseT	UTP	100m	Cat5e upwards
1000BaseSX	MMF	550m	SC Connector
1000BaseCX	Balanced Shielded Copper	25m	Special Connector
1000BaseLX	MMF/SMF	550m (Multi) /2000m(Single)	SC and LC Connector

ETHERNET OVER OTHER STANDARDS

- Ethernet over Power Line (Broadband over Power Line (BPL))
- Ethernet over HDMI

COMMON ETHERNET CABLE TYPES

Ethernet Name	Cable Type	Max Distance	Notes
10GBaseT	UTP	100m	
10GBaseSR	MMF	300m	
10GBaseLR	SMF	10km	
10GBaseER	SMF	40km	
10GBaseSW	MMF	300m	
10GBaseLW	SMF	10km	Used with SONET
10GBaseEW	SMF	40km	

MODULE 5:NETWORK DEVICES

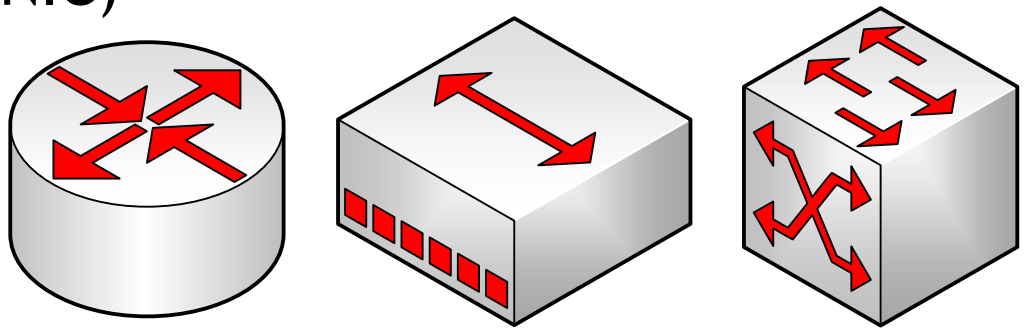
NETWORK+ 007

Your fastest way to learn. Guaranteed.

FIREBRAND

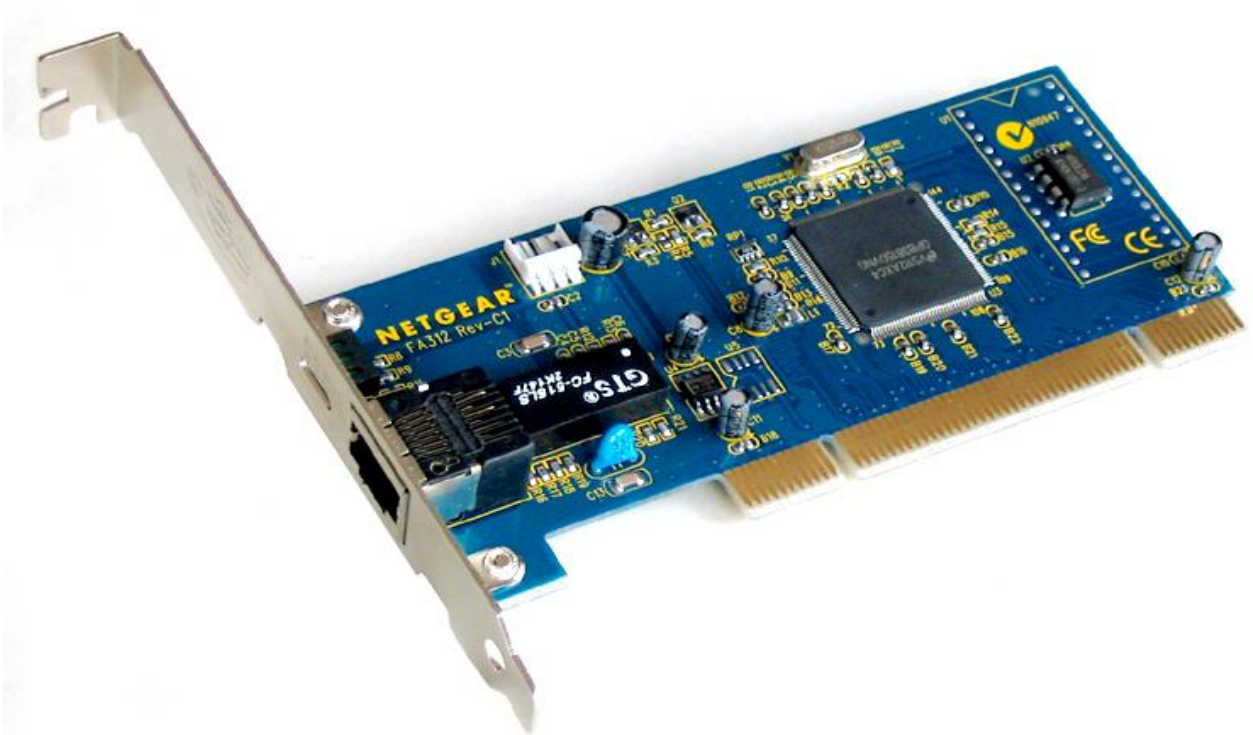
COMMON NETWORK DEVICES

- Network Interface Card (NIC)
- Hub
- Bridge
- Switch
- Router
- Firewall
- Intrusion Detection System (IDS)
- Intrusion Prevention System (IPS)
- Access Point



NETWORK INTERFACE CARD (NIC)

Unique identifier – Media Access Control address (MAC)



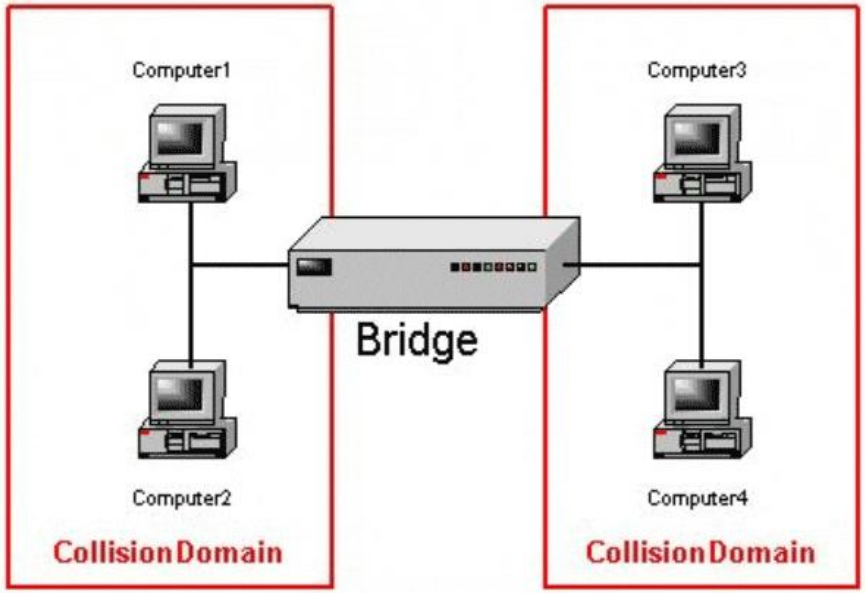
HUBS AND REPEATER – LAYER 1 DEVICES

HUB enables a number of nodes to connect to a network (one per port)

REPEATER retransmit signals (may clean and strengthen the signal) to increase distances between nodes

BRIDGE – LAYER 2 DEVICE

A **BRIDGE** (or 'Transparent Bridge') connects two similar network segments together. Its primary function is to keep traffic separated on either side of the bridge, breaking up Collision Domains within a single Broadcast Domain

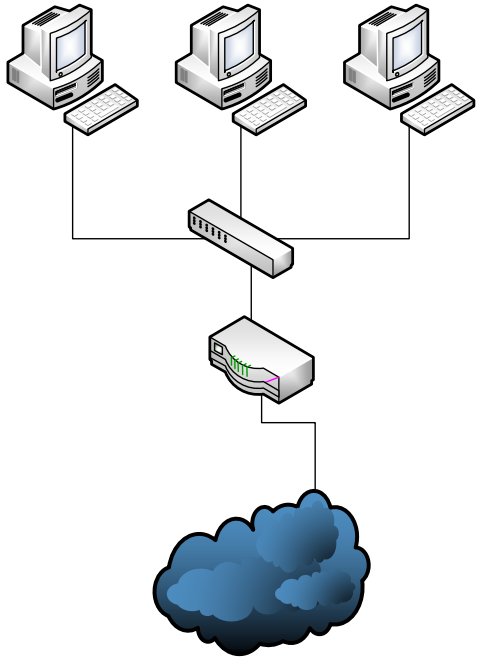


SWITCH – LAYER 2 DEVICE

- Multiport bridges
- Operate at DATALINK layer
- Control collision domains
- Now used extensively instead of Hubs and Bridges
- May also incorporate LAYER 3 technology (VLAN)

ROUTER – LAYER 3 DEVICE

Traditional LAYER 3 device (NETWORK Layer)
Forwarding based upon network layer IP address
Control Broadcast and Collision Domains
Can use multiple routing protocols

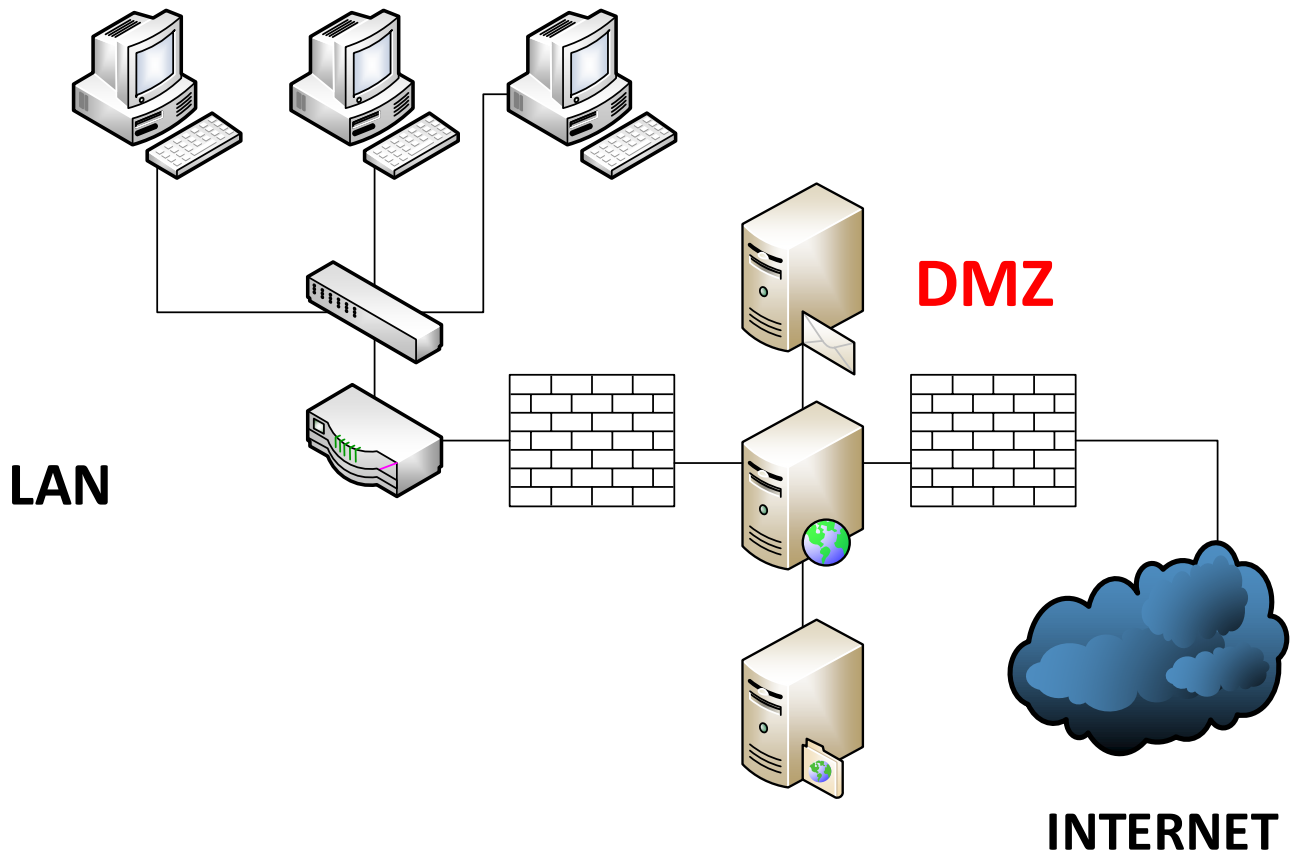


FIREWALL

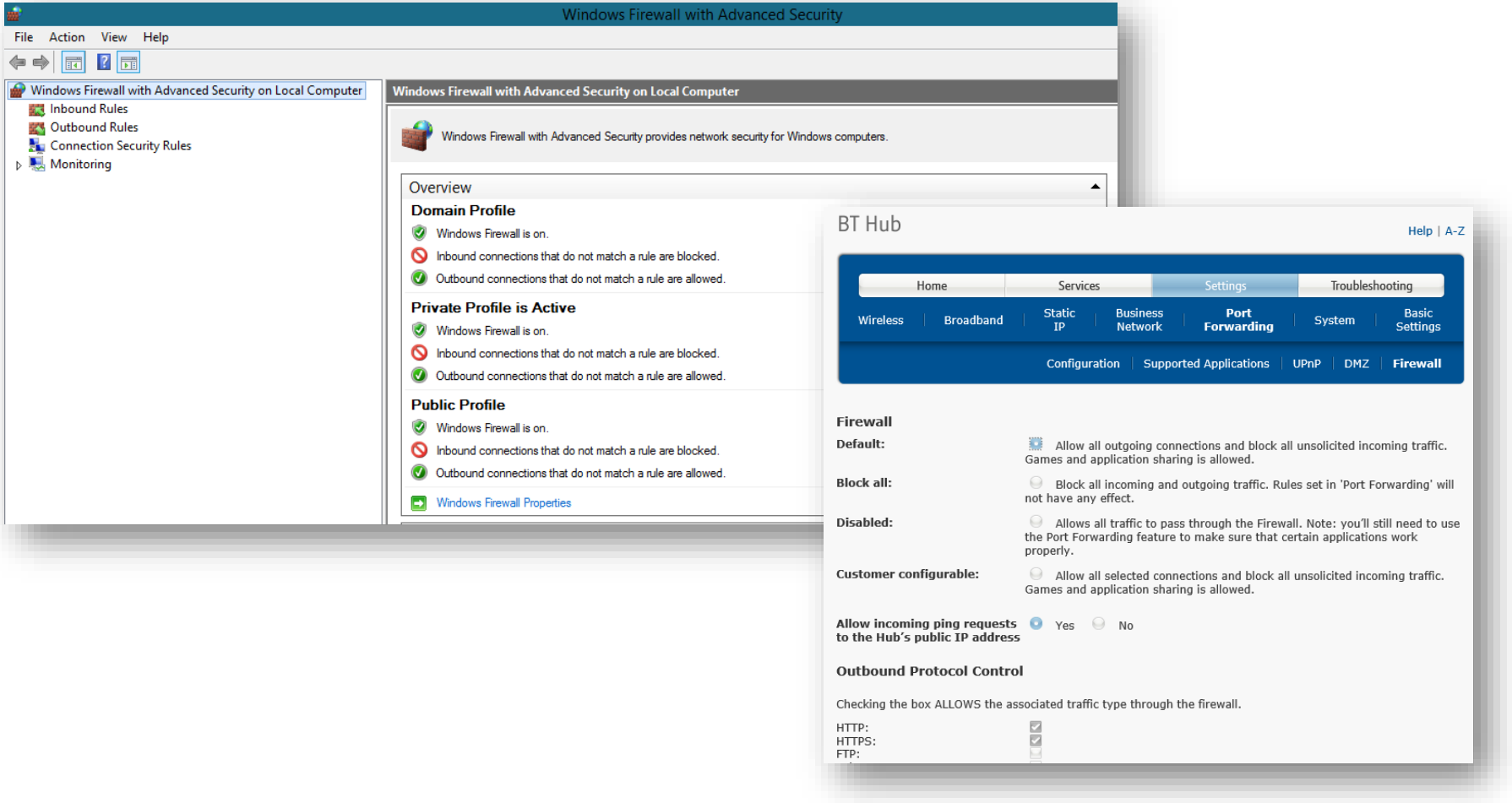
- Provide the first layer of defence in network security
- May be hardware or software (or both)
- Based on configuration rules
- Used to established Demilitarised Zones (DMZ)

FIREWALLS - DMZ

Used to protect the LAN from External attacks/intrusion



FIREWALL - RULES



IDS/IPS

Intrusion Detection System (IDS)

- **Host Based (HIDS) or Network Based (NIDS)**
- **Passive Monitoring**
- Anomaly Detection
- Signature Detection
- Heuristics

Intrusion Protection System

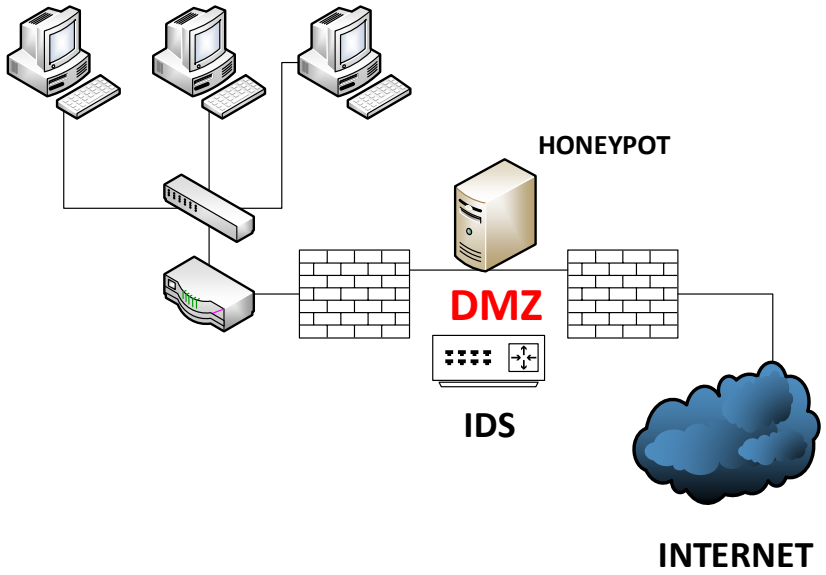
- **Host Based (HIPS) or Network Based (NIPS)**
- **Active Monitoring**

IDS/IPS

Honeypot / Honeynet

Used to monitor intrusion / attacks and conduct intelligence gathering

Used to deflect potential attacks

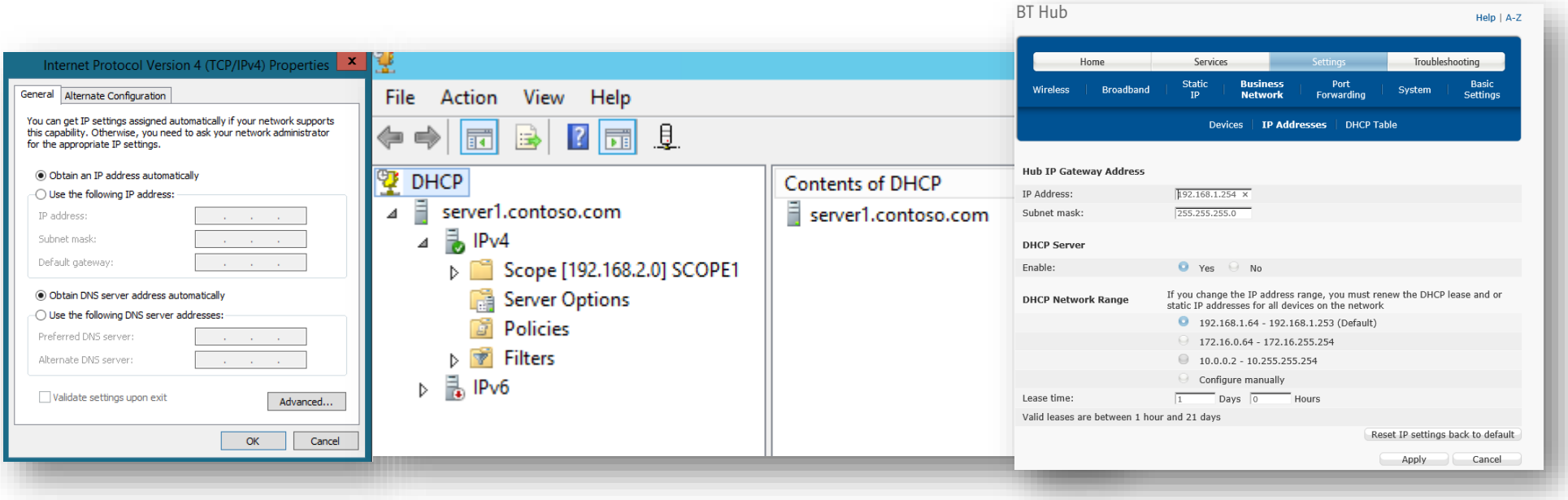


WIRELESS ACCESS POINTS (WAP)

- Connects computers with wireless adapters to a network
- Access Point is a translational bridge
- 802.11b/g Access Points use **CSMA/CD** to connect to network (LAN) and **CSMA/CA** to communicate with other wireless devices

DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP)

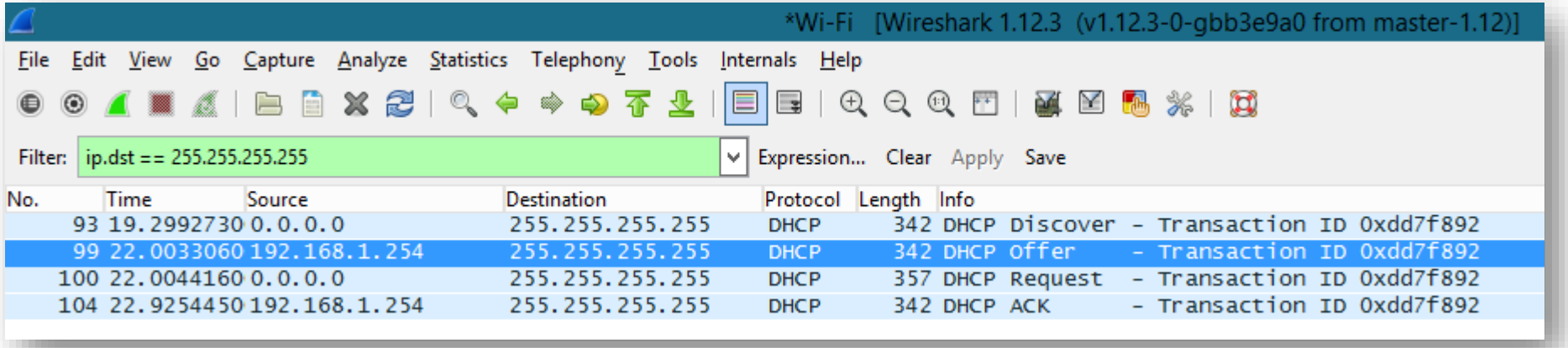
Dedicated Server Role or Integrated with Network Device



DHCP

DHCP Client sends Broadcast packets to DHCP Server in order to acquire an IP address from the DHCP Scope (DORA)

- DHCP **D**iscover
- DHCP **O**ffer
- DHCP **R**equest
- DHCP **A**ck



DHCP SETTINGS

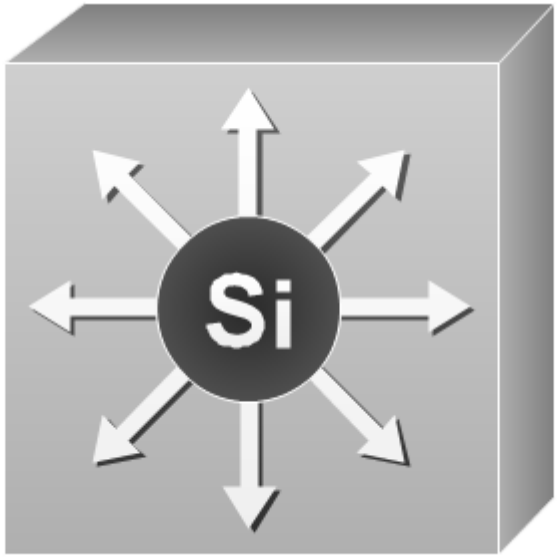
- Reservations (set on MAC address of client)
- Exclusions (used for statically assigned clients)
- Authorised on the network
- IP helper – client unable to receive address information
- Scope must be activated
- Clients will default to APIPA (169) address if no DHCP available
- Internet Connection Sharing (ICS) includes DHCP service

SPECIALISED NETWORK DEVICES

Multilayer Switch (MLS)

Works at Layer 2 and Layer 3 (Routing)

Very popular devices



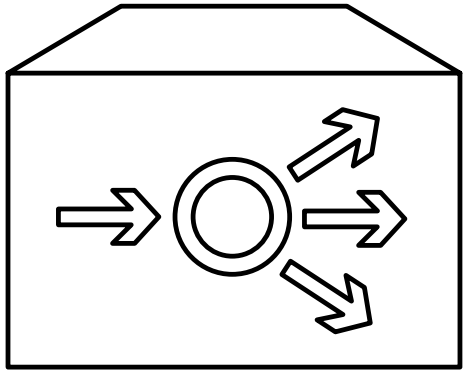
SPECIALISED NETWORK DEVICES

Load Balancer

Fault Tolerance / Redundancy

Used to support servers such as:

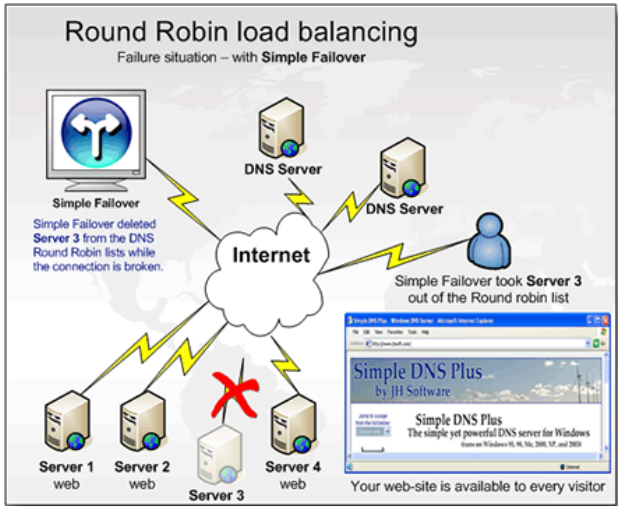
- Web Servers
- FTP Servers
- Remote Desktop Servers
- VPN Servers
- Single node failure
- All nodes fail
- Intermittent connection



ROUND ROBIN

Essentially this is a simple mechanism in which the content access request is responded to by the load balance in a rotational basis.

Geographically distributed web servers are best served by applying DNS load balancing round robin server content distribution. As an example a company can have a single domain name and four absolutely identical company home pages on four physical servers based in Europe, Asia, North America and Africa.



DNS ROUND ROBIN

DNS round robin load balancing has one major advantage, it is extremely simple to implement, but it needs to be understood that it does have a number of potentially important drawbacks. These come from the very DNS hierarchy that it uses to perform its load balancing.

Load balancers use smart techniques to measure and respond to TTL times they will try to maintain a connection with a server to complete a user session using caching and TTL even if the server in question is failing and about to be unable to continue to service the network users.

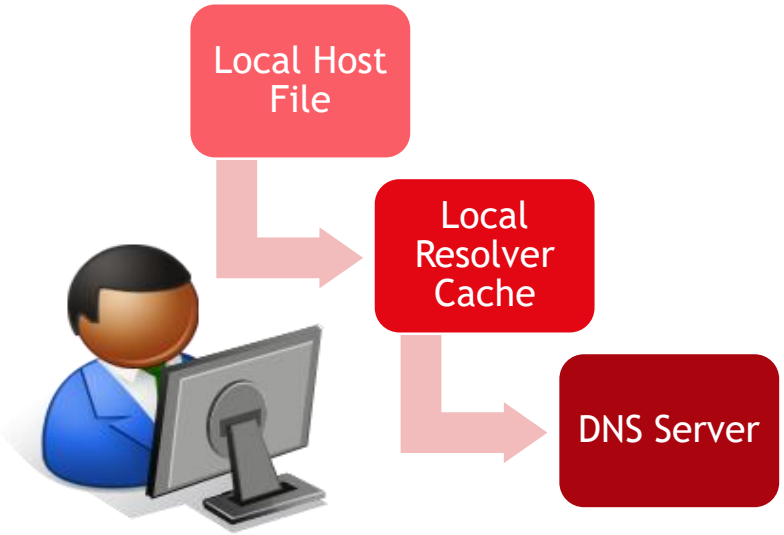
This problem can result in unpredictability and even corrupt the DNS tables. This means that servers that have failed continue to receive requests for providing content to users despite the fact that they are down and therefore no longer available.

DOMAIN NAMING SYSTEM (DNS)

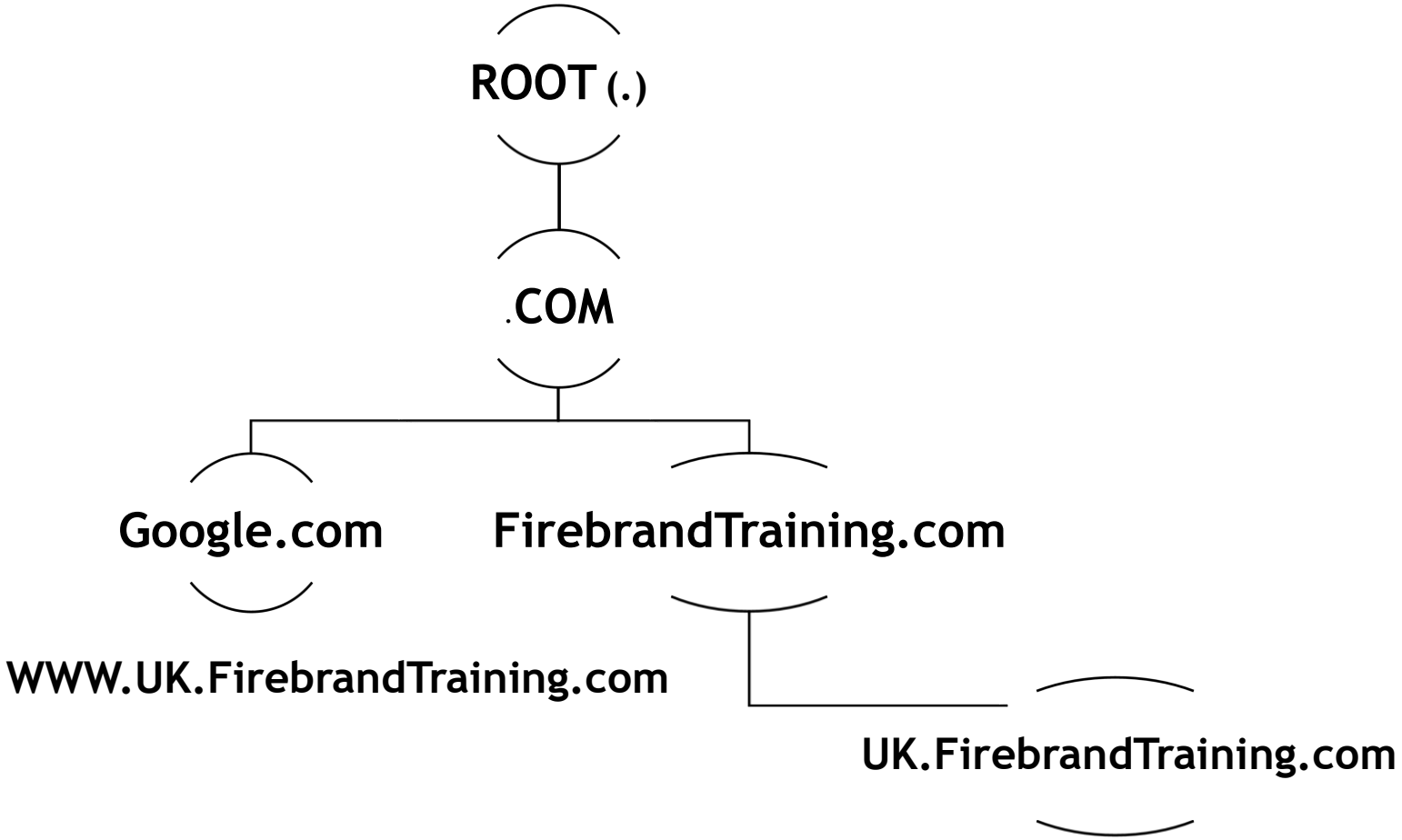
- Resolves FQDN to IP addresses (Forward Lookup)
- Resolves IP addresses to FQDN (Reverse Lookup)
- DNS entries held in a database on a server called a Zone
- Zone is an area of contiguous namespace for which a DNS server is authoritative
- DNS Server is able to Forward requests and Cache responses in support of clients

DNS RESOLUTION

Host File
Local Resolver Cache
DNS
NetBios Cache
WINS
Broadcast
LMHosts



DNS ON THE INTERNET



DNS RECORDS

RECORD	INFO
A	Host Record (IPv4)
AAAA	Host Record (IPv6)
PTR	Reverse Lookup Record
NS	Named Server Record (DNS Server)
MX	Mail Exchange (Email Server)
Alias (Cname)	Used to point friendly name records to other hosts
SOA	Start of Authority (controls DNS Zone transfers and records)
SRV	Service Locator records (eg. location of Domain Controllers and associated services)

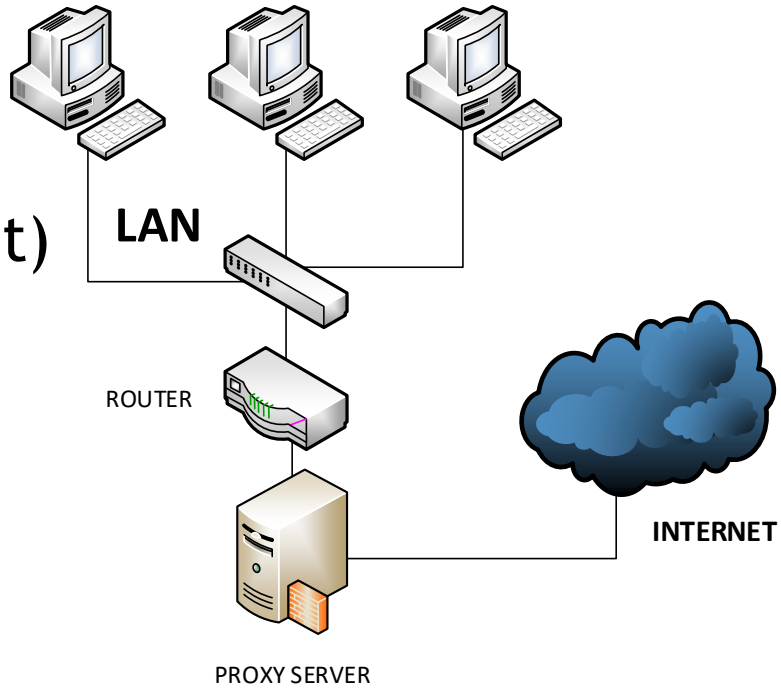
SPECIALISED NETWORK DEVICES

Proxy Server

Two main types:

- Caching Proxy
- Web Proxy

Reverse proxy (incoming from the Internet)



SPECIALISED NETWORK DEVICES

PACKET SHAPER (TRAFFIC SHAPER)

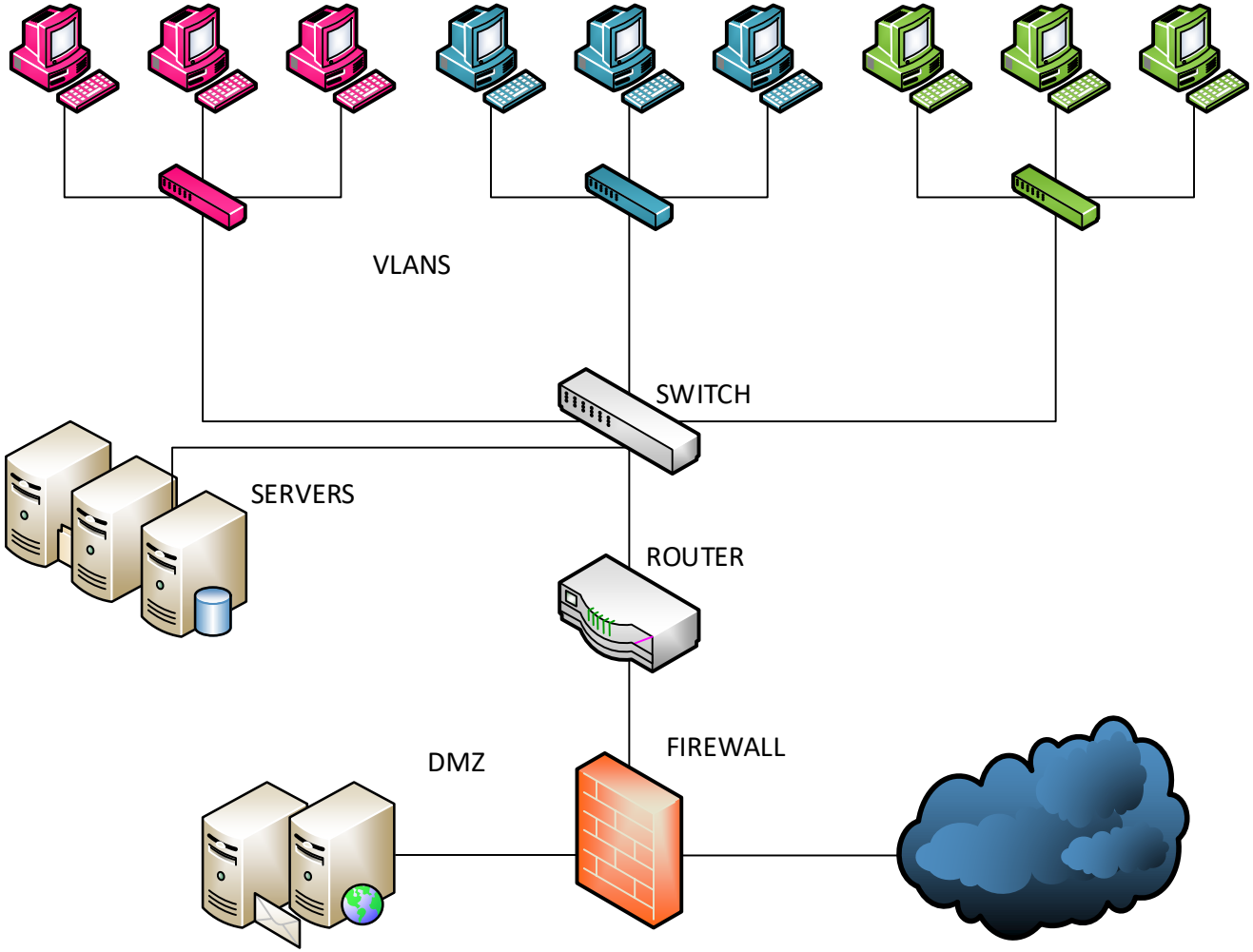
- Allow for traffic management (bandwidth)
- Set against network profile
- May work with Quality of Service (QOS) configurations

SPECIALISED NETWORK DEVICES

VPN CONCENTRATOR

Dedicated device to handle multiple VPN (Virtual Private Network) connections and associated configurations

BASIC NETWORK DEVICE LAYOUT



NETWORK DOCUMENTATION

Label and Tag everything
- System, port, circuit, patch panel

Physical and logical maps
- What does you network look like – network plan

Baseline
- How does the network and traffic flow look normally

Cable management
- ANSI/TIA/EIA 606

Change management
- How do you manage any changes to the network i.e. equipment upgrades

MODULE 6:TCP/IP

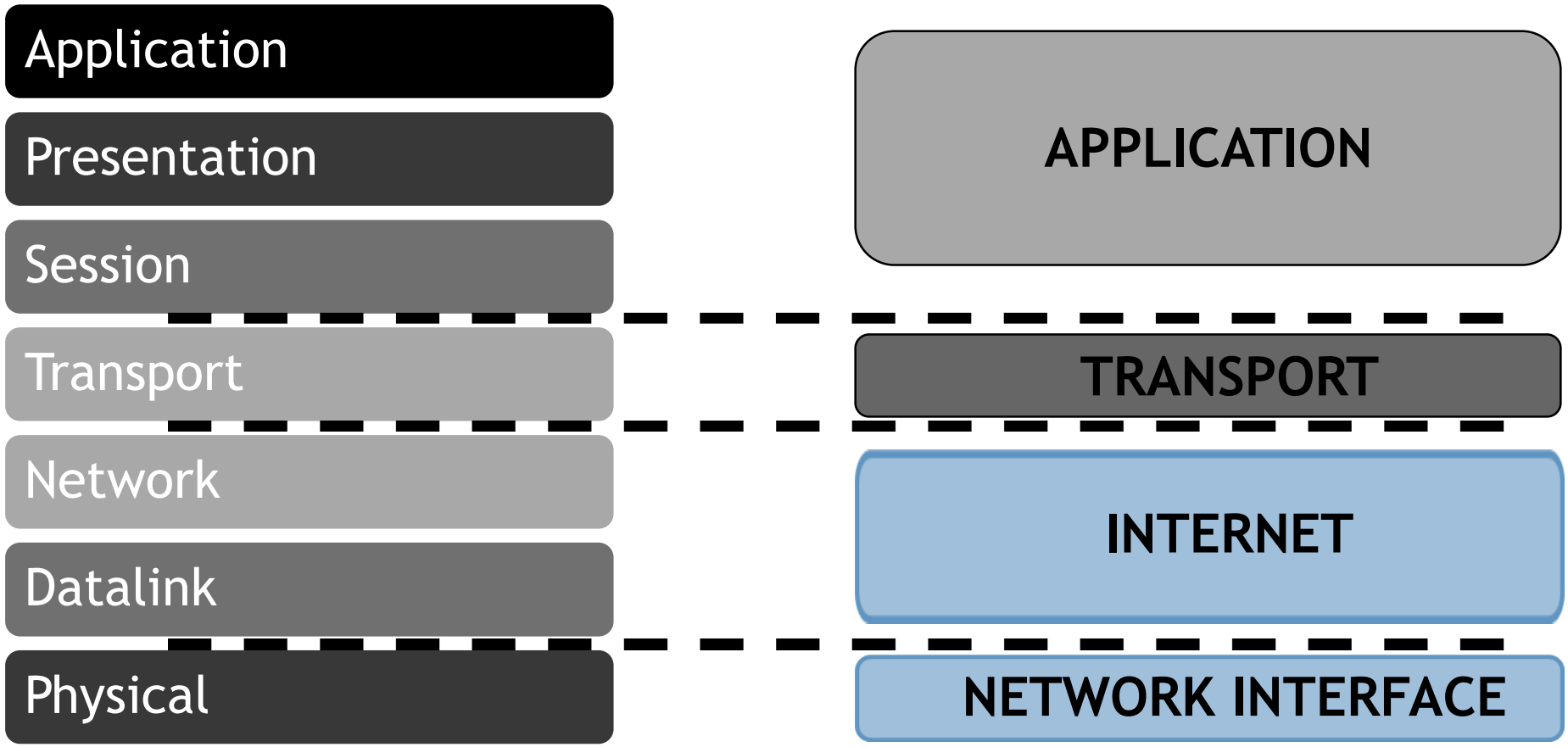
NETWORK+ 007

13/03/2019

Your fastest way to learn. Guaranteed.

FIREBRAND

DEPARTMENT OF DEFENSE (DOD) TCP/IP MODEL



PORTS

- Allow applications or protocols to use specific values for connections
- Range from 0-65535
- 0-1023 are reserved for specified TCP/IP applications and are known as “Well Known Ports”
- Destination and Source port numbers
- Sockets include IP address and Port Number

LOTS OF PORTS

- Non-ephemeral ports –permanent port numbers. Ports 0 through 1,023, usually on a server or service
- Ephemeral ports – temporary port numbers
- Ports 1,024 through 65,536
- Determined in real-time by the clients

PORT RULES

- TCP and UDP ports can be any number between 0 and 65,535
- Most servers (services) use non-ephemeral (not-temporary) port numbers. You can have non standard ports
- Port numbers are for communication
- Around 1000 commonly used ports

PORT NUMBERS

Application Layer Protocol	Port (s)	Transport Protocol
FTP File Transport Protocol	20/21	TCP
TELNET	23	TCP
SSH	22	TCP
DNS	53	TCP/UDP
DHCP	67/68	UDP
TFTP	69	UDP
HTTP	80	TCP
HTTPS	443	TCP
SMTP	25	TCP

PORT NUMBERS

Application Layer Protocol	Port Number (s)	Transport Protocol
NETBIOS	137,138,139	TCP
LDAP	389	TCP
IGMP	463	UDP
Secure LDAP	636	TCP
RDP	3389	TCP
NTP	123	UDP
NNTP	119	UDP
POP3	110	TCP
IMAP4	143	TCP
SNMP	161	UDP

INTERNET LAYER PROTOCOLS

- Internet Protocol (IP)
- Internet Control Message Protocol (ICMP)
- Address Resolution Protocol (ARP)

INTRODUCTION TO IP

- Logistics
- Efficiently move large amounts of data
- Use a shipping truck where the truck is the IP and the container stores the data
- The network topology is the road
- Ethernet, DSL, coax cable
- The truck is the Internet Protocol (IP)
- The boxes inside the truck container hold your data which can be made up of TCP and UDP
- Inside these boxes is the data you need to send via ‘DHL’

TRANSPORT PROTOCOLS

Transmission Control Protocol (TCP)

- Connection Orientated
- TCP Three Way Handshake – Syn, Syn-Ack, Ack
- Error correction – resend packet
- Flow control - the receiver can manage how much data is sent

User Datagram Protocol (UDP)

- Connection-less – send the data out and you hope it arrives
- Used for streaming media, DNS and VOIP
- No formal open or close to the connection
- No error correction
- No flow control - sender determines the amount of data transmitted

IP

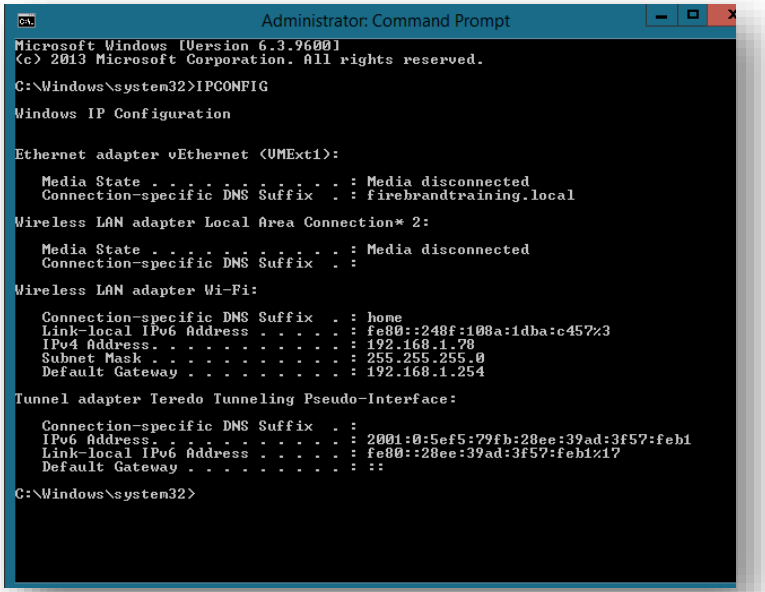
IPv4

IPv6

Windows Clients use dual stack

Command Line Utilities:

- IPCONFIG
- IFCONFIG (Linux/Unix)

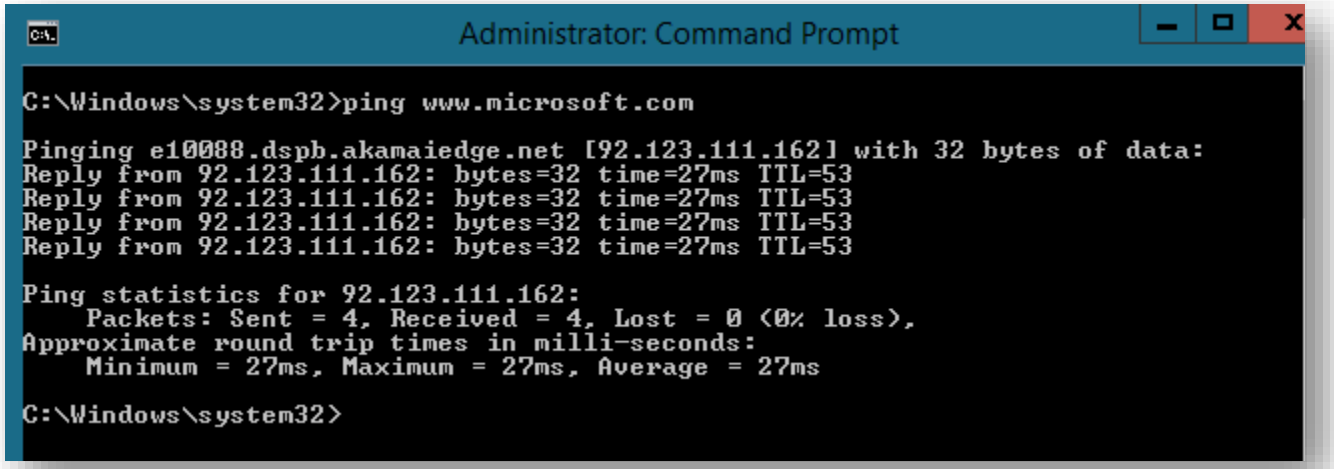


ICMP

Management and messaging for IP

Command line utilities:

- PING
- PATHPING
- TRACERT

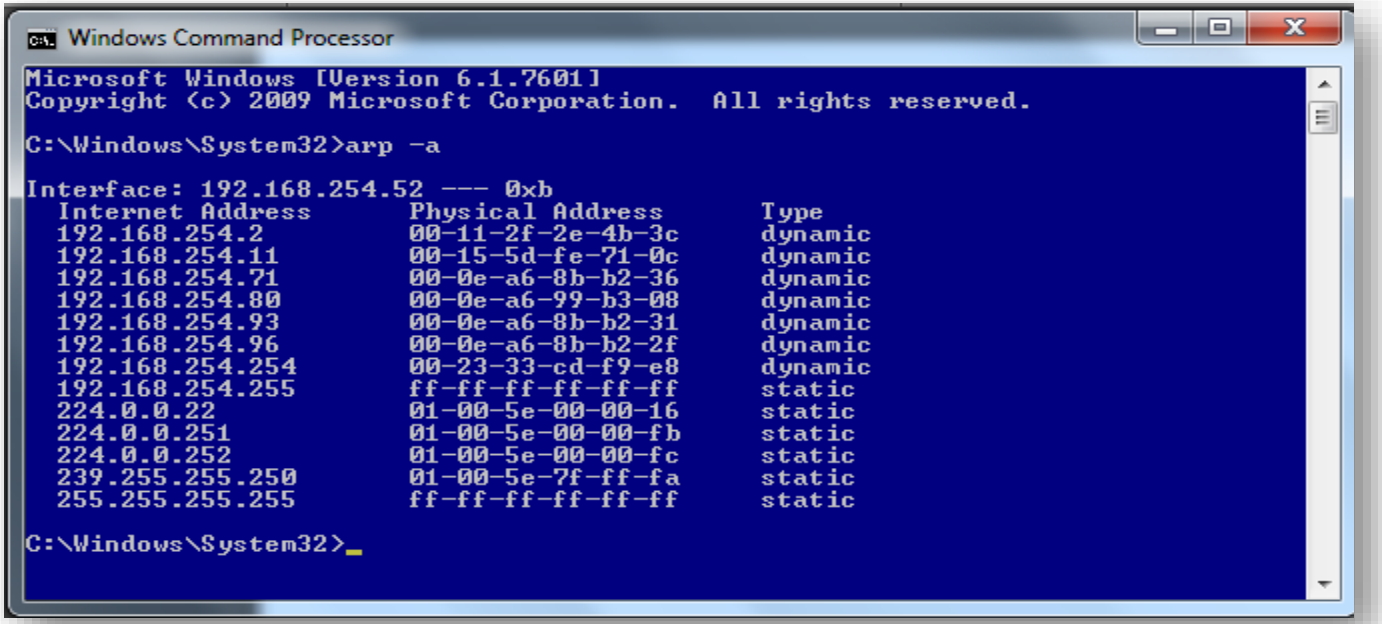


ARP

Address Resolution Protocol

IP to MAC Address

Reverse ARP (RARP) resolves IP from MAC address



MODULE 7:IP ADDRESSING

NETWORK+ 007

Your fastest way to learn. Guaranteed.

FIREBRAND

INTERNET PROTOCOL (IP)

IPv4

32 Bit Address Scheme

Divided into Network Address and Host

Subnet Mask

Broken in 4 Octets (8 bits)

Represented by dotted-decimal notation

Eg. 192.168.2.200 / 24

Or 192.168.2.200

255.255.255.0

BINARY TO DECIMAL

To convert binary to decimal the easiest method is use a number line and matching 1 and 0 to the line:

128 64 32 16 8 4 2 1

1 1 0 0 1 1 0 1

The binary number 11001101 converted is:

128 + 64 + 8 + 4 + 1 = 205

Try converting **10100110** and **00001111**

HEXADECIMAL

DENARY	BINARY	HEX
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	0001	8
9	1001	9
10	0110	A
11	1011	B
12	0011	C
13	1011	D
14	0111	E
15	1111	f

BINARY TO HEX CONVERSION

Let the fun commence…

11001100

Break number into a nibble (4 bits)

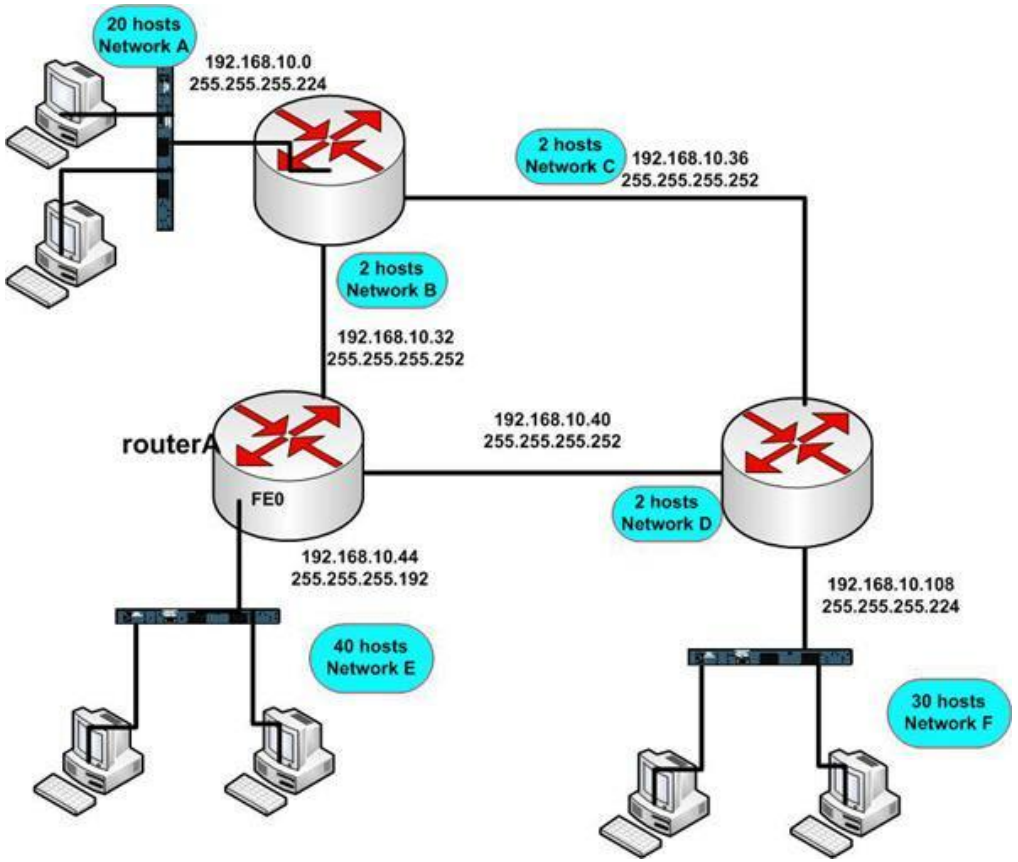
1100 = 12 = C, 1100 = 12 therefore Hex is **0xCC** (Ox to denote it is a hex value)

Try converting **10110101** to HEX and then decimal

SUBNETTING

The word subnet is short for sub network—a smaller network within a larger one. It allows us to make efficient use of IP addresses by allocating them in blocks.

Subnets have a beginning and an ending, and the beginning number is always even and the ending number is always odd. The beginning number is the "Network ID" and the ending number is the "Broadcast ID." You're not allowed to use these numbers because they both have special meaning with special purposes.



CDIR (CLASSLESS INTER DOMAIN ROUTING)

IP addresses are assigned to networks in different sized ‘blocks'. The size of the ‘block' assigned is written after an oblique (/), which shows the number of IP addresses contained in that block.

For example, if an Internet Service Provider (ISP) is assigned a “/16”, they receive around 64,000 IPv4 addresses. A “/26” network provides 64 IPv4 addresses. The **lower** the number after the / (oblique), the more addresses contained in that “block”.

SUBNET MASK

A subnet mask is a bitmask that encodes the prefix length in quad-dotted notation: 32 bits, starting with a number of 1 bits equal to the prefix length, ending with 0 bits, and encoded in four-part dotted-decimal format: 255.255.255.0.

1st Octet		2nd Octet		3rd Octet		4th Octet
255	.	255	.	255	.	0

CIDR (CLASSLESS INTER DOMAIN ROUTING)

Class	Address	# of Hosts	Netmask (Binary)	Netmask (Decimal)
CIDR	/21	2,048	11111111 11111111 11111000 00000000	255.255.248.0
CIDR	/22	1,024	11111111 11111111 11111100 00000000	255.255.252.0
CIDR	/23	512	11111111 11111111 11111110 00000000	255.255.254.0
C	/24	256	11111111 11111111 11111111 00000000	255.255.255.0
CIDR	/25	128	11111111 11111111 11111111 10000000	255.255.255.128
CIDR	/26	64	11111111 11111111 11111111 11000000	255.255.255.192
CIDR	/27	32	11111111 11111111 11111111 11100000	255.255.255.224
CIDR	/28	16	11111111 11111111 11111111 11110000	255.255.255.240
CIDR	/29	8	11111111 11111111 11111111 11111000	255.255.255.248
CIDR	/30	4	11111111 11111111 11111111 11111100	255.255.255.252

SUBNETTING

PUBLIC and PRIVATE address ranges allocated by IANA (Class-full Addressing)

PUBLIC Ranges: (Routable on the Internet)

Class	Range	Hosts
A	1-126 / 8	16,777, 214
B	128-191 /16	65,534
C	192-223	254
D	224-239	Multicast
E	240-254	Development

IP

Private Ranges: (Not routable on the Internet)

Class	Range
A	10.0.0.0-10.255.255.255
B	172.16.0.0-172.31.255.255
C	192.168.0.0-192.168.255.255

APIPA – Automatic Private IP Address

169.254.X.X	255.255.0.0

IPV6

134 undecillion addresses

128 bit Address Range

Displayed in hexadecimal format of eight 16bit groups, separated by a colon (:)

Eg: **4002:0da4:72a3:0025:0000:6e53:0430:4241**

May also be written as:

4002:da4:72a3:25::6e53:430:4241

(lead zeros removed)

IPV6

- Double stack IPv4 runs with IPv6
- IPv6 tunnelling
- 6 to 4 to run IPv6 over IPv4 network
- Teredo for Linux or open source Miredo
- Tunnel IPv6 through NAT IPv4

NDP

NDP (Neighbour Discovery Protocol) operates at the link layer of the Internet model and gathers various information required for internet communication.

Router Solicitation (RS) - Hosts inquire with RS messages to locate routers on an attached link.

Router Advertisement (RA) Routers advertise their presence together. Using various link and Internet parameters either periodically, or in response to a RS

Neighbour Solicitation (NS) - Neighbour solicitations are used to determine the link layer address of a neighbour, or to verify that a neighbour is still reachable via a cached link layer address.

Neighbour Advertisement (NA) - Neighbour advertisements are used by nodes to respond to a Neighbour Solicitation message.

Redirect - Routers may inform hosts of a better first hop router for a destination.

IPV6 CONFIGURATION

Finding Router

- ICMPv6 (ICMP port needs to be open for IPv6) adds the NDP routers, also sends unsolicited RA messages
- From the multicast destination of ff02::1 transfers IPv6 address information.
- Sent as a multicast NA to replace ARP (IPv4 only) to find MAC a address.

ASSIGNING IPV6 ADDRESSES

- Static addressing can be useful as the IP address never change (think servers). The MAC address changes and Extended Unique Identifier (64-bit)
- We can use the 48 bit Mac address to form part of the IPv6 address
- We need to add to the 48 bit Mac address to make it 64 bit

Conversion process

- Split the MAC into two 3-byte (24 bit) halves and put **FFFE** in the middle (the missing 16 bits)
- Invert the **seventh** bit which changes the address from globally unique/universal and turns the burned-in address (BIA) into a locally administered address.

IPV6 ADDRESSES

Unicast – one to one (Same as IPv4)

Multicast – one to many (Similar to IPv4)

Anycast – one to one of many (Unique to IPv6)

IPV6

Unicast Addresses:

- **Global Unicast** *(similar to Public IPv4 addresses)*
- **Link Local Unicast** *(similar to APIPA IPv4 addresses)*
- **Unique Local Unicast** *(similar to Private IPv4 addresses)*

SPECIAL IPV6 ADDRESSES

Loopback Address

::1 (127.0.0.1)

Link Local Addresses

FE80:: (Similar to APIPA addresses)

ICMPV6

Replaces IGMP with **Multicast Listener Discovery (MLD)**

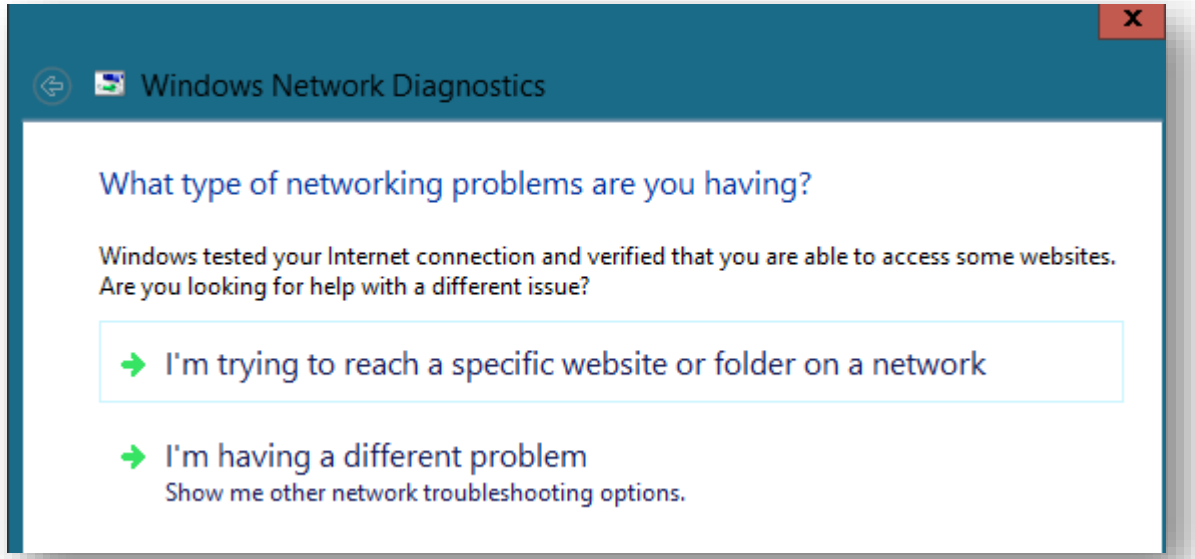
Replaces ARP with **Neighbour Discovery (ND)**

TROUBLESHOOTING IP

Physical Network Components (NIC, Cables, Switches, Routers)

Network Interface Card Configuration

- IPCONFIG
- PING
- TRACERT
- ARP

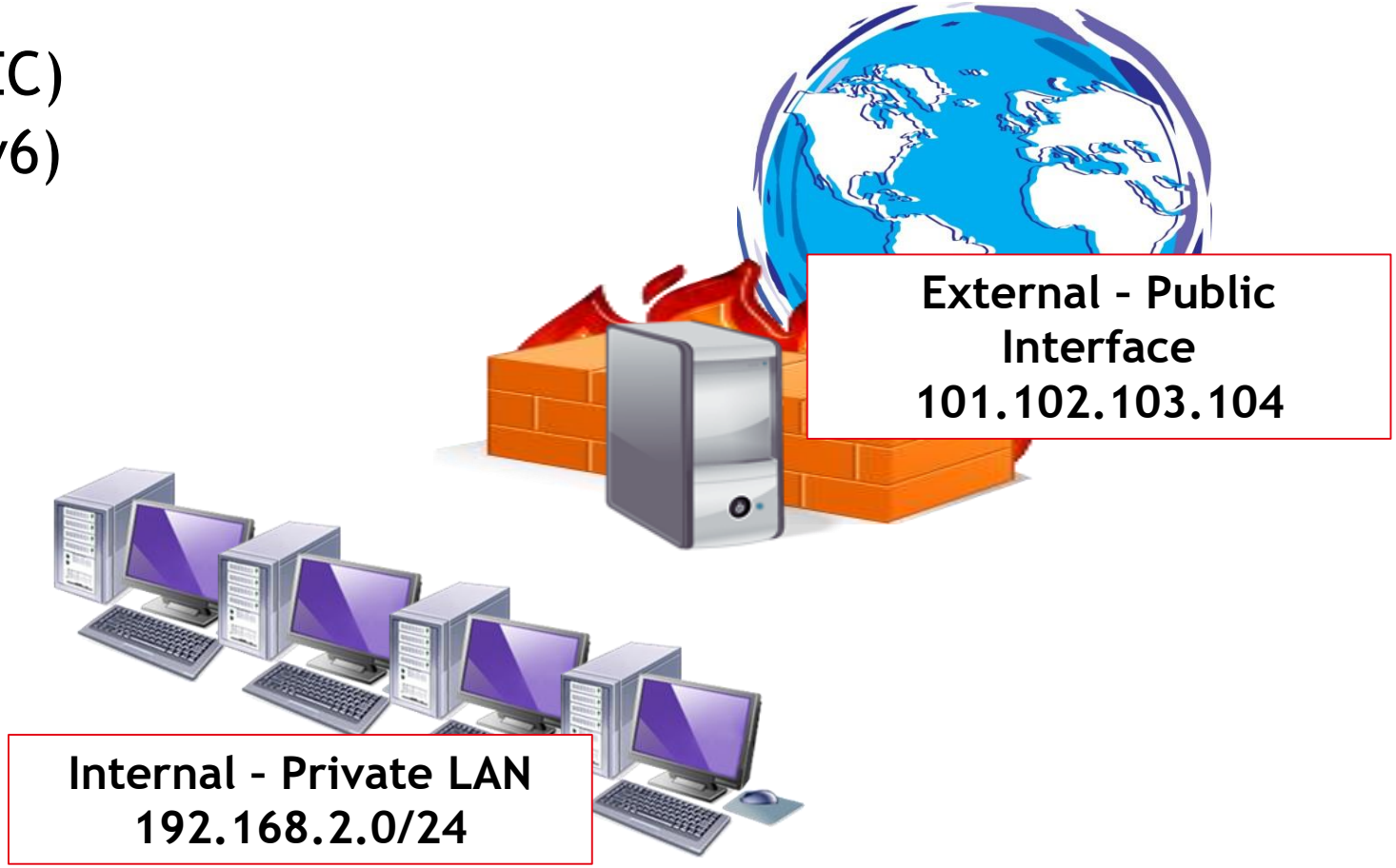


NETWORK ADDRESS TRANSLATION (NAT)

- NAT allows for the continuation of private IPv4 addressing
- Translates between Private and Public IP networks (different to Routing)
- Simply replaces the source IP address (private) with that of the external (public) IP address to enable routing on the Internet
- Addition security features (Firewall)

NAT

Basic NAT
NAT-T (IPSEC)
NAT-PT (IPv6)



MODULE 8: ROUTING

NETWORK+ 007

Your fastest way to learn. Guaranteed.

FIREBRAND

ROUTING TABLES

Routing table provides the router with a ‘map’ of the network configuration and where it can receive and send packets to/from

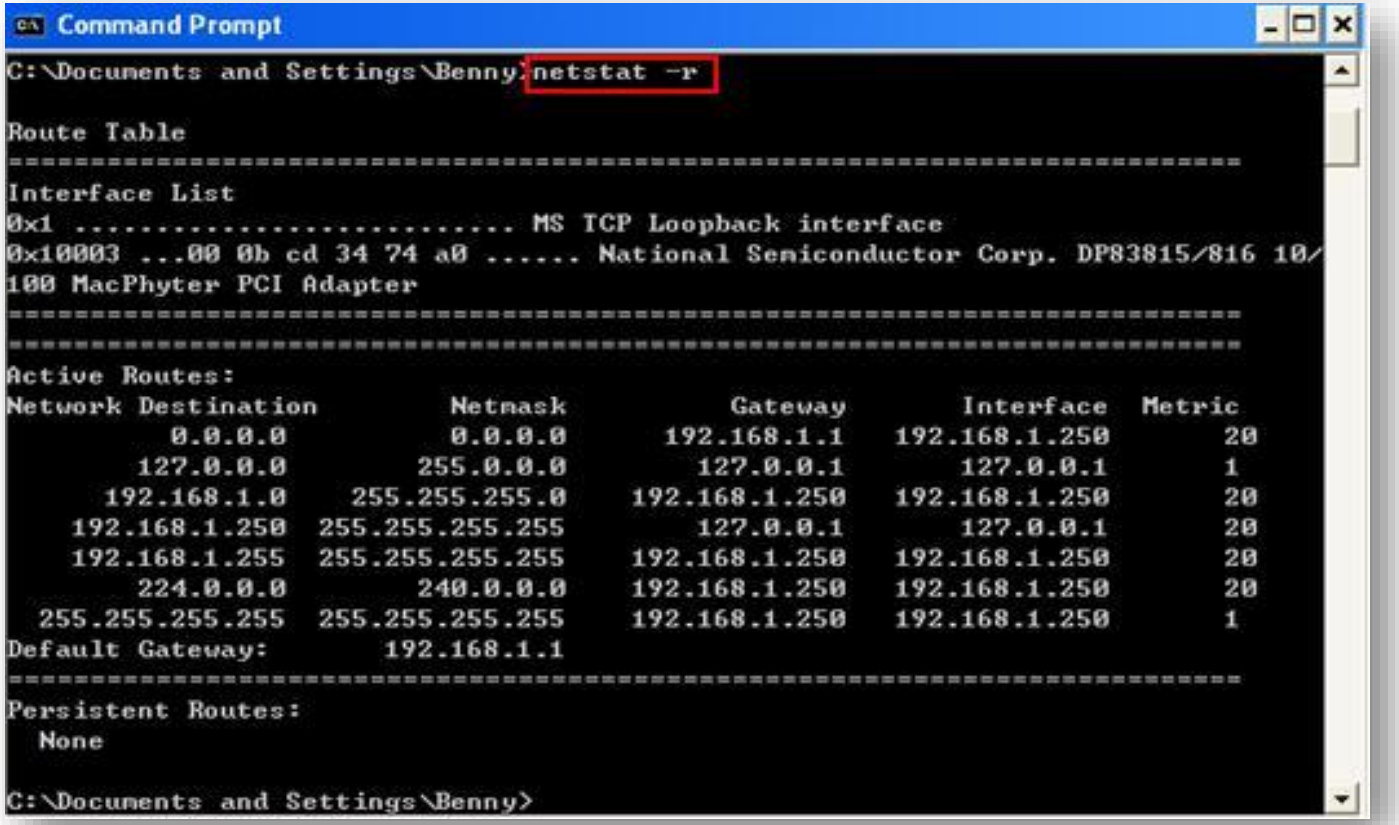
Typically routing table includes:

- Destination addresses
- Gateway locations
- Interfaces
- Cost (Metric)

WINDOWS ROUTING TABLE

Route Print

Netstat -r



ROUTING INFORMATION

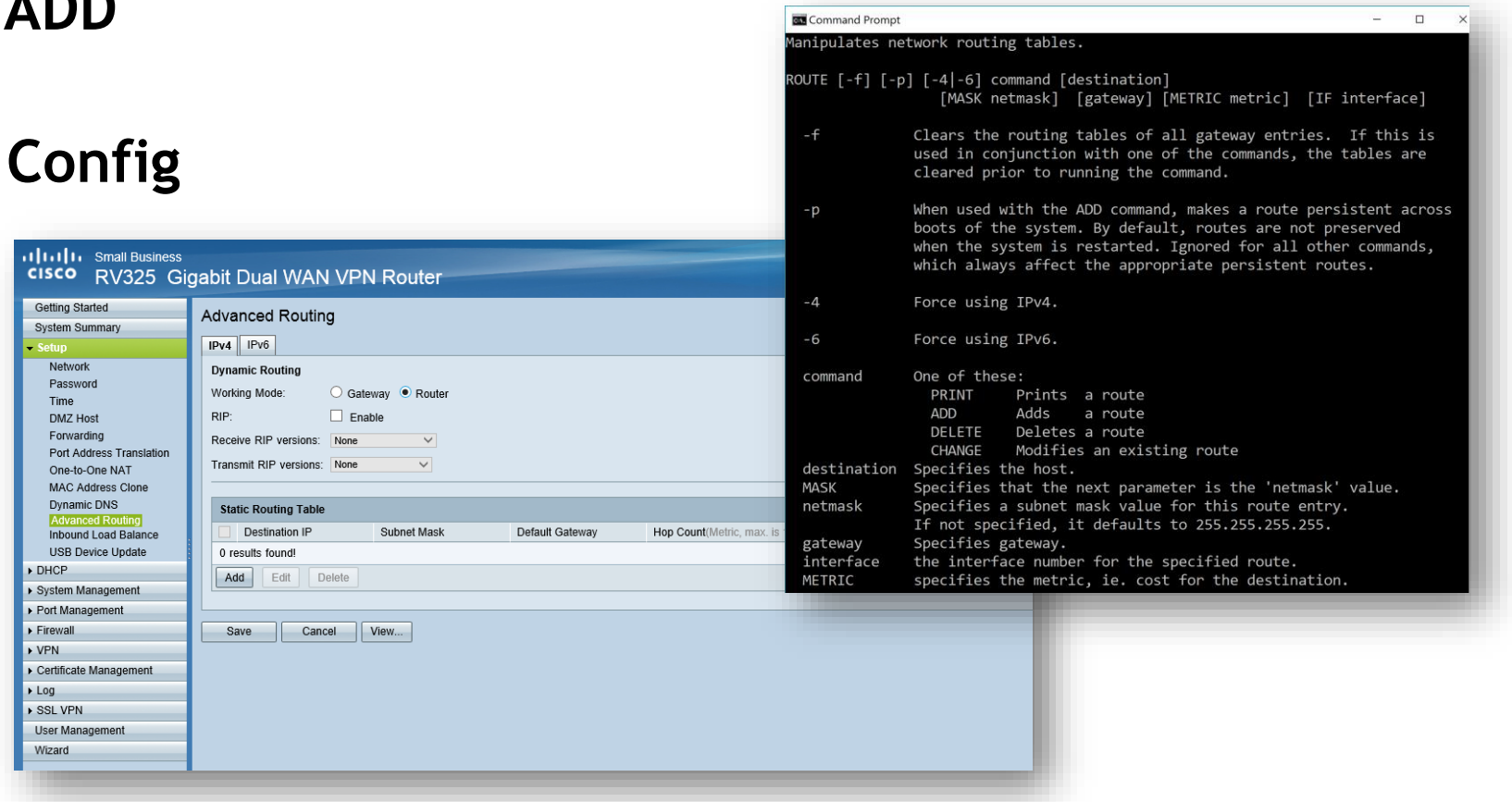
Routing Tables are updated by:

- STATIC Routing (Routing information is manually configured)
- DYNAMIC Routing (Routing protocols automatically update routing information)

STATIC ROUTING

ROUTE ADD

Router Config



DYNAMIC ROUTING

Routing Protocols

Distance Vector

- Use algorithms to calculate best routes based on distance (cost) and direction (vector)
- Transfer the whole routing table to other routers (up to a maximum number of hops)
- Routing tables are broadcast at regular intervals
- Used for small/medium size networks

DISTANT VECTOR ROUTING PROTOCOLS

Routing Internet Protocol (**RIP**)v1

RIPv2 – increased security (authentication)

BGP Border Gateway Protocol (BGP) – used to connect Autonomous Systems (AS) across the Internet but is actually a hybrid protocol

(Autonomous Systems use classes of routing protocols Interior and Exterior Gateway Protocol (IGP and EGP)) Is often put as distant vector however…

BGP

BGP is a path vector protocol is a network routing protocol which maintains the path information that gets updated dynamically. Updates which have looped through the network and returned to the same node are easily detected and discarded.

It is different from the distance vector routing and link state routing. Each entry in the routing table contains the destination network, the next router and the path to reach the destination.

Think of it as a **HYBRID** routing protocol

DYNAMIC ROUTING PROTOCOLS

Link State - router has to be on to connect

Open Shortest Path First (OSPF)

More common IGP (OSPFv2 for IPv4, OSPFv3 for IPv6)

IS-IS (Intermediate System - Intermediate System)

LINK AGGREGATION (LACP)

The advantages of link aggregation in contrast with conventional connections using an individual cable include:

- higher potential transmission speed
- higher accessibility

LINK AGGREGATION RULES

All of the aggregated links must:

- Be in full duplex mode
- Use the same data transmission rates (at least 1 Gbit/s)
- Use parallel point-to-point connections
- Connect to precisely one endpoint on a switch or server. Won't work on multiple switches.

LINK AGGREGATION CONTROL PROTOCOL (LACP)

LACP allows the exchange of information with regard to the link aggregation between the two members. This information is packetized in Link Aggregation Control Protocol Data Units (LACDUs).

Each individual port can be configured as an active or passive LACP using the control protocol.

Passive LACP: the port prefers not transmitting LACPDUs. The port will only transmit LACPDUs when its counterpart uses active LACP (preference not to speak unless spoken to).

Active LACP: the port prefers to transmit LACPDUs and thereby to speak the protocol, regardless of whether its counterpart uses passive LACP or not (preference to speak regardless).

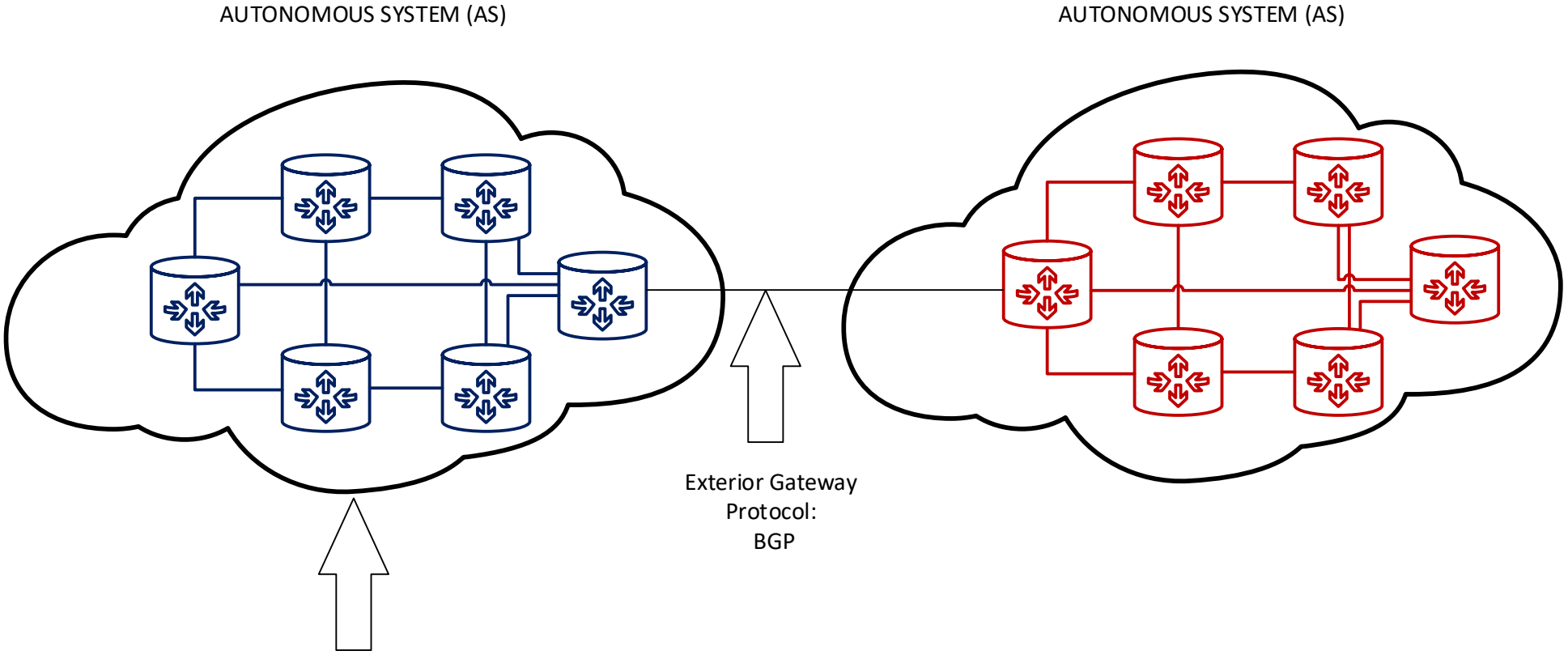
LINK AGGREGATION CONTROL PROTOCOL (LACP)

In contrast to a static link aggregation, LACP provides the following advantages:

- Even if one physical links fails, it will detect if the point-to-point connection is using a media converter, so that the link status at the switching port remains up. Because LACPDUs do not form a component of this connection, the link will be removed from the link aggregate. This ensures that packets will not be lost due to the failed link.

- Both of the devices can mutually confirm the LAG configuration. With static link aggregation, errors in the configuration or wiring will often not be detected as quickly.

ROUTING PROTOCOLS



HIGH AVAILABILITY ROUTING

Use of ‘Virtual Routers’

Hot Standby Router Protocol (HSRP) – Cisco proprietary

Virtual Router Redundancy Protocol (VRRP)

IPV6 DYNAMIC ROUTING

RIPng
EIGRPv6
OSPFv3

MODULE 9: SWITICHING & VLANS

NETWORK+ 007

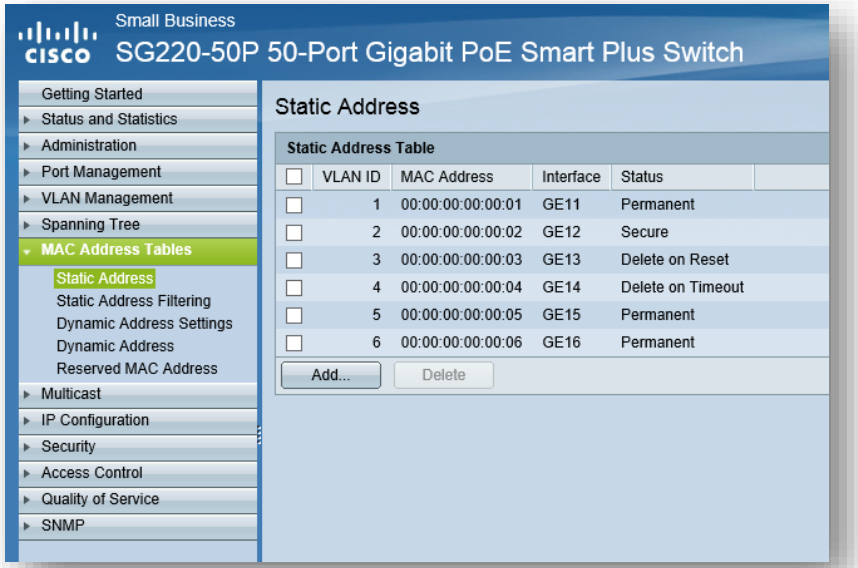
Your fastest way to learn. Guaranteed.

FIREBRAND

SWITCHES

LAYER 2 Device

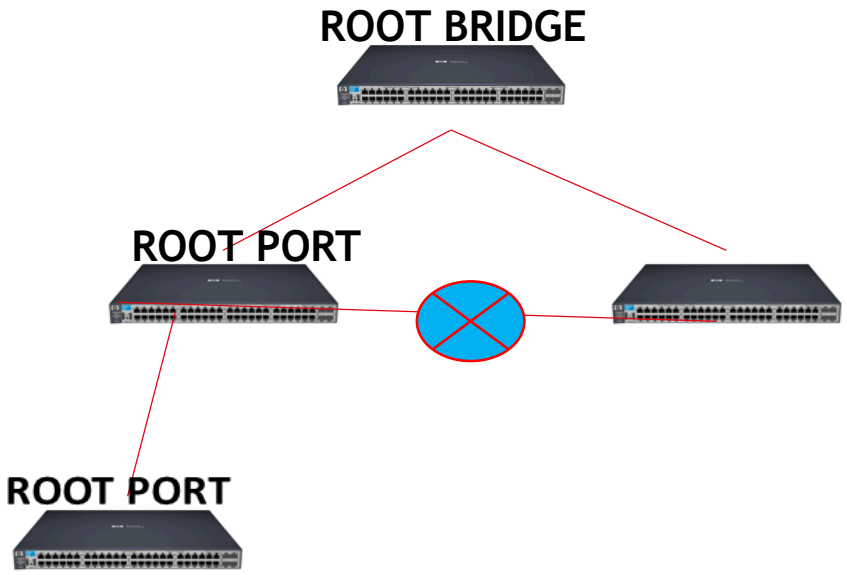
- Used to create separate collision domains
- Managed or Unmanaged devices
- Learn the MAC address of host locations using MAC address forward/filter table



SPANNING TREE PROTOCOL (STP)

Eliminates bridging loops (aka switching loops)

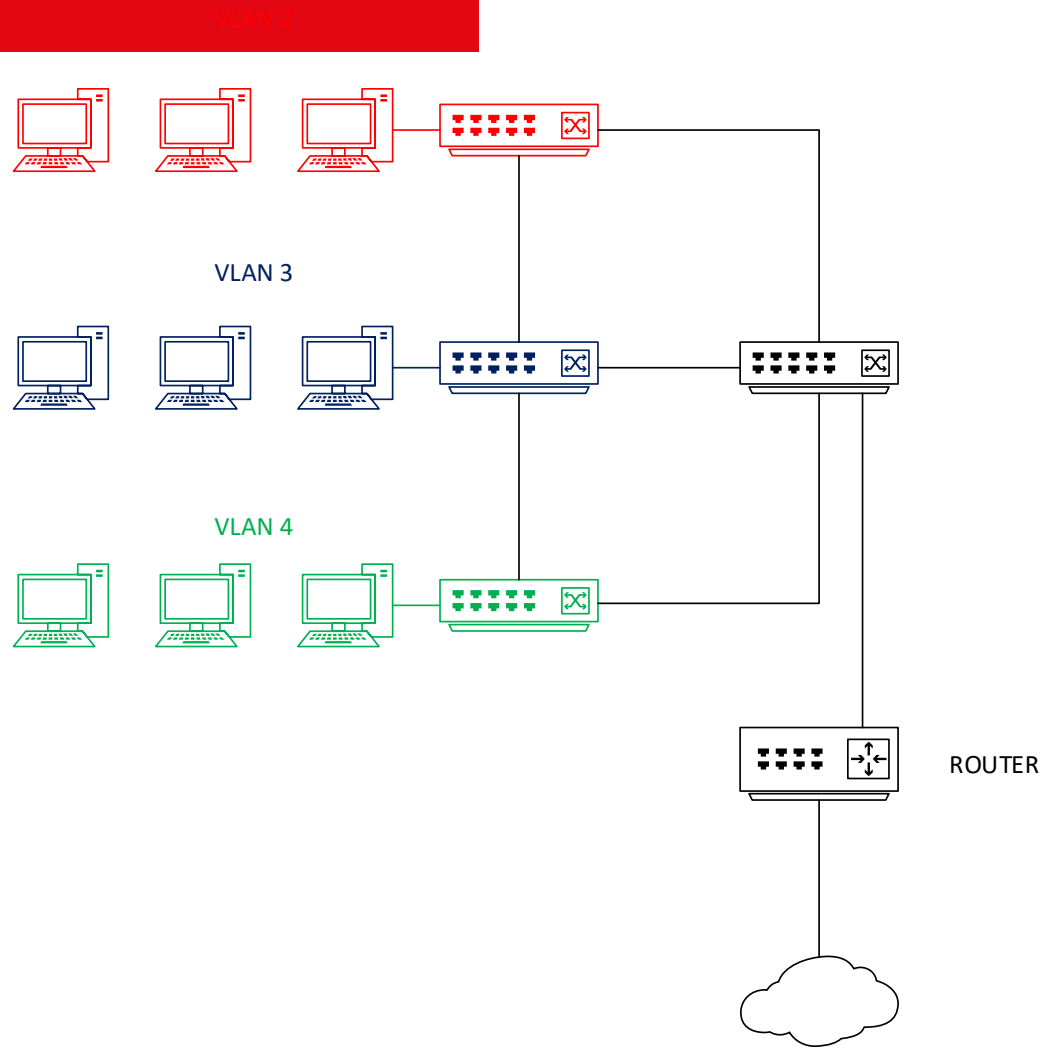
Enables switches to detect loops, communicate with other switches and block potential loops taking place



VIRTUAL LAN (VLAN)

- Switches provide a method of broadcast domain segmentation called Virtual LANs (VLANs)
- Layer 2 method of creating more broadcast domains
- VLANs logically divide a switch into multiple, independent switches at Layer 2, each in their own broadcast domain

VIRTUAL LAN (VLAN)

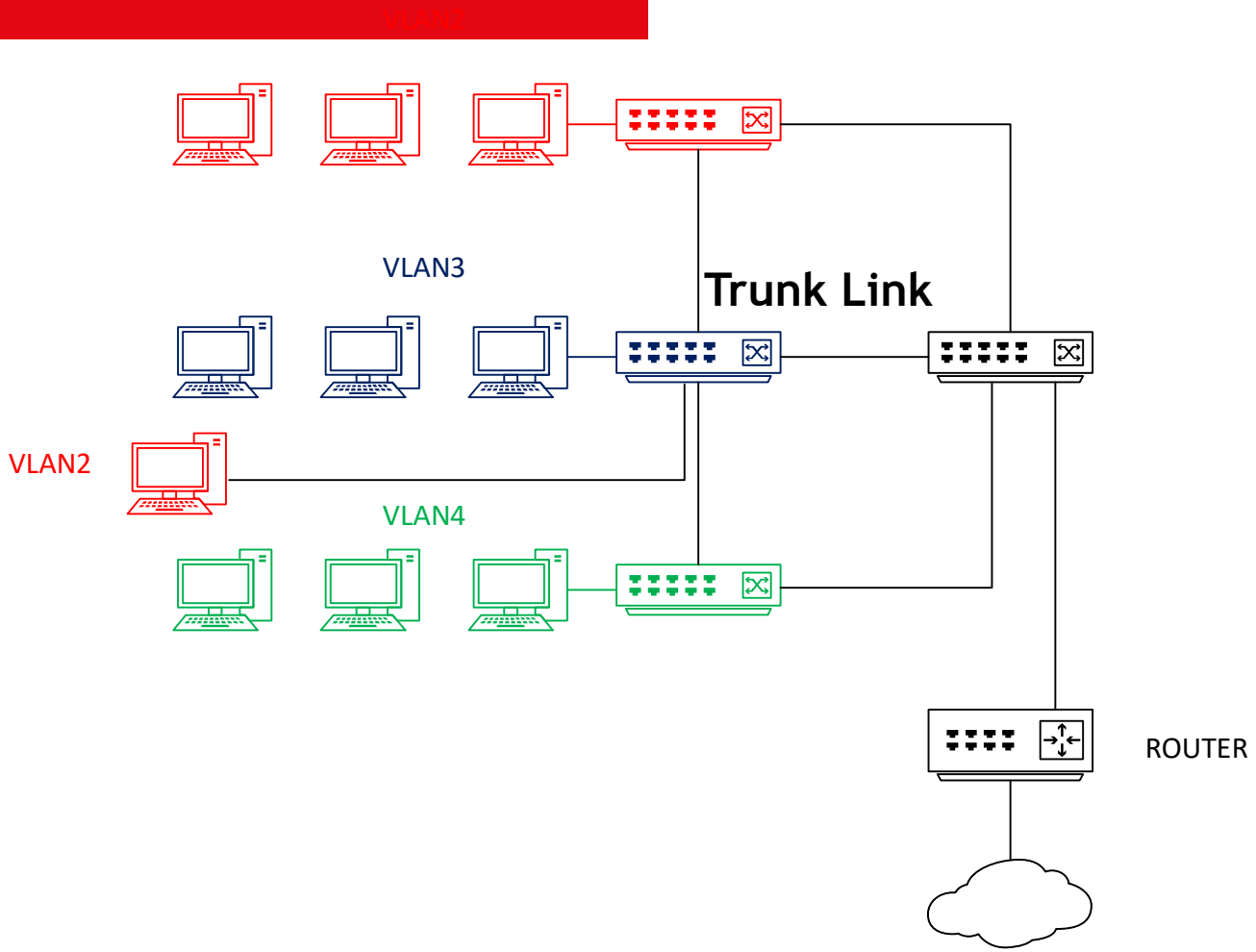


VLANS

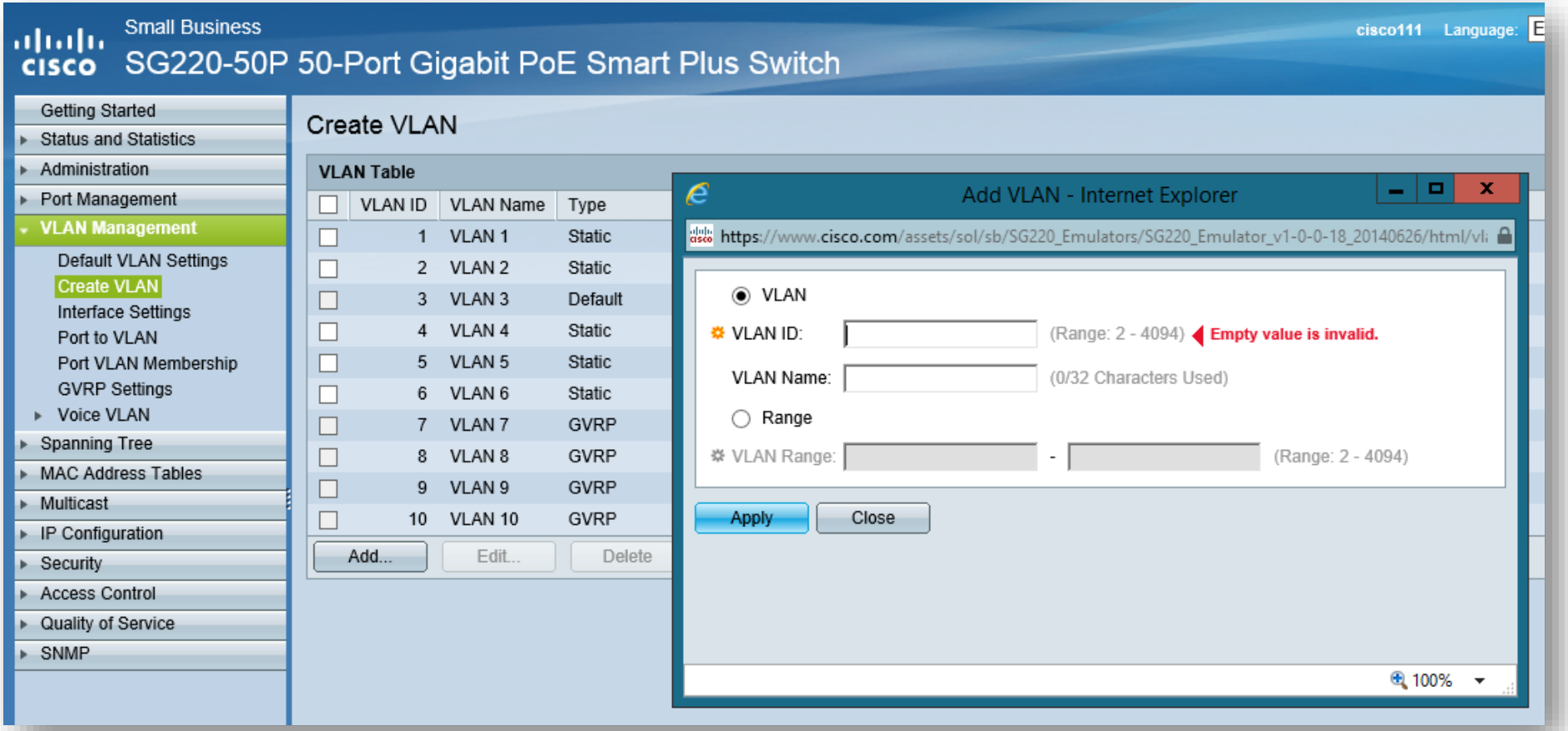
Each VLAN behaves as if it were a separate switch

- Packets are forwarded only to ports on that VLAN
- VLANS require a **TRUNK** to span multiple switches VLAN Trunking Protocol (VTP)
- manages VLANs across a switched internetwork and maintains consistency throughout that network
- A port can be assigned to a given VLAN

VLAN



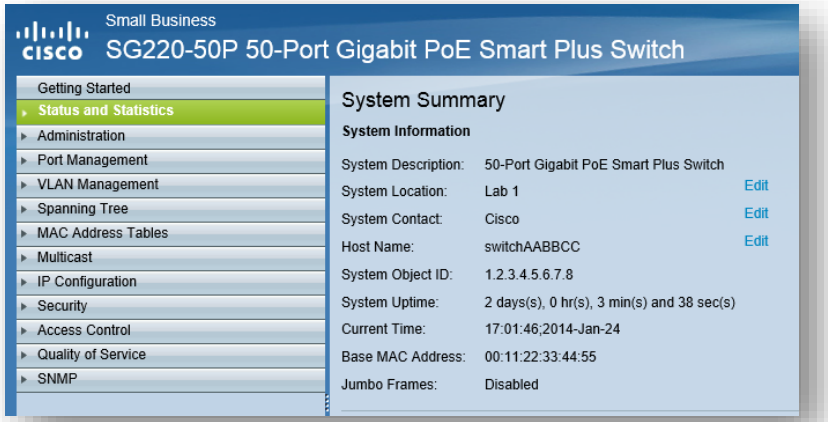
VLAN



ADDITIONAL SWITCH SETTINGS/PROPERTIES

Dependant upon the type/manufacture of the device

- Quality of Service (QOS) – set DSCP values (Differentiated Services Code Point)
- Port Security
- Port Mirroring
- Port Bonding
- Flood Guards
- Multicasting
- Power over Ethernet (PoE) 802.3af/802.3at



NTP (NETWORK TIME PROTOCOL – PORT 123)

- Switches, routers, firewalls, servers, workstations every device has its own clock. Synchronizing the clocks becomes critical for log files, authentication information, outage details and automatically.
- Accuracy is better than 1 millisecond on a local network
- Without system time synchronisation how will you follow what is happening across various devices via their logs if they are not in time.
- Ever used CCTV and there is a time offset, so the time you have does not match the time on the CCTV!

NETWORK TIME PROTOCOL

NTP stratum layers

- Stratum is how far the time signal is from the source clock
- Stratum 0 - Atomic clock, GPS clock
- Stratum 1 - Synchronized to stratum 0 servers primary time servers
- Stratum 2 - Sync'd to stratum 1 servers

Configuring NTP (port 123)

- specify the NTP server address (IP or hostname) you can use multiple NTP servers for redundancy (availability).

MODULE 10: WIRELESS NETWORKING

NETWORK+ 007

13/03/2019

Your fastest way to learn. Guaranteed.

FIREBRAND

802.11 STANDARDS

Standard	Max Throughput	Frequency	Notes
802.11a	54Mbps	5GHz	
802.11b	11Mbps	2.4GHz	
802.11g	54Mbps	2.4GHz	
802.11n	Up to 600Mbps	2.4/5GHz	MIMO
802.11ac	Up to 1Gbps	5GHz	MIMO

WLAN SETUP

Ad hoc mode

Wireless clients connect to each other without an AP

Infrastructure mode

- Clients connect through an AP through one of two modes
- BSSid (Basic Service Set ID) uses one AP
- ESSid (Extended Service Set ID) More than one access point exists

WIRELESS COMPONENTS

Wireless Access Point (WAP)
Wireless NIC
Wireless LAN (WLAN) Controller

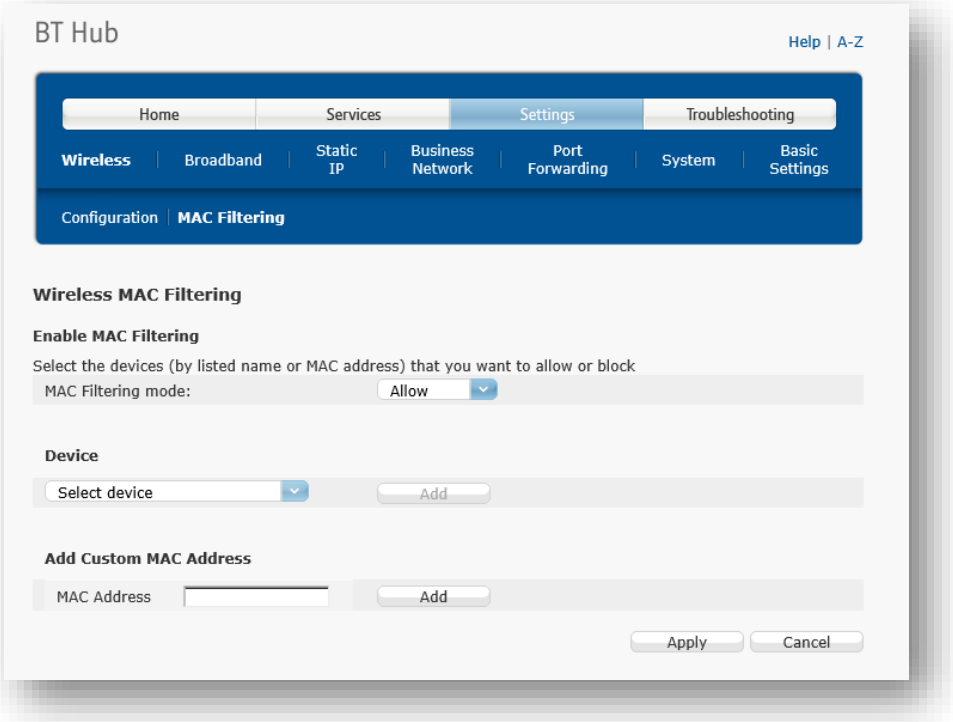
WIRELESS SECURITY

Threats

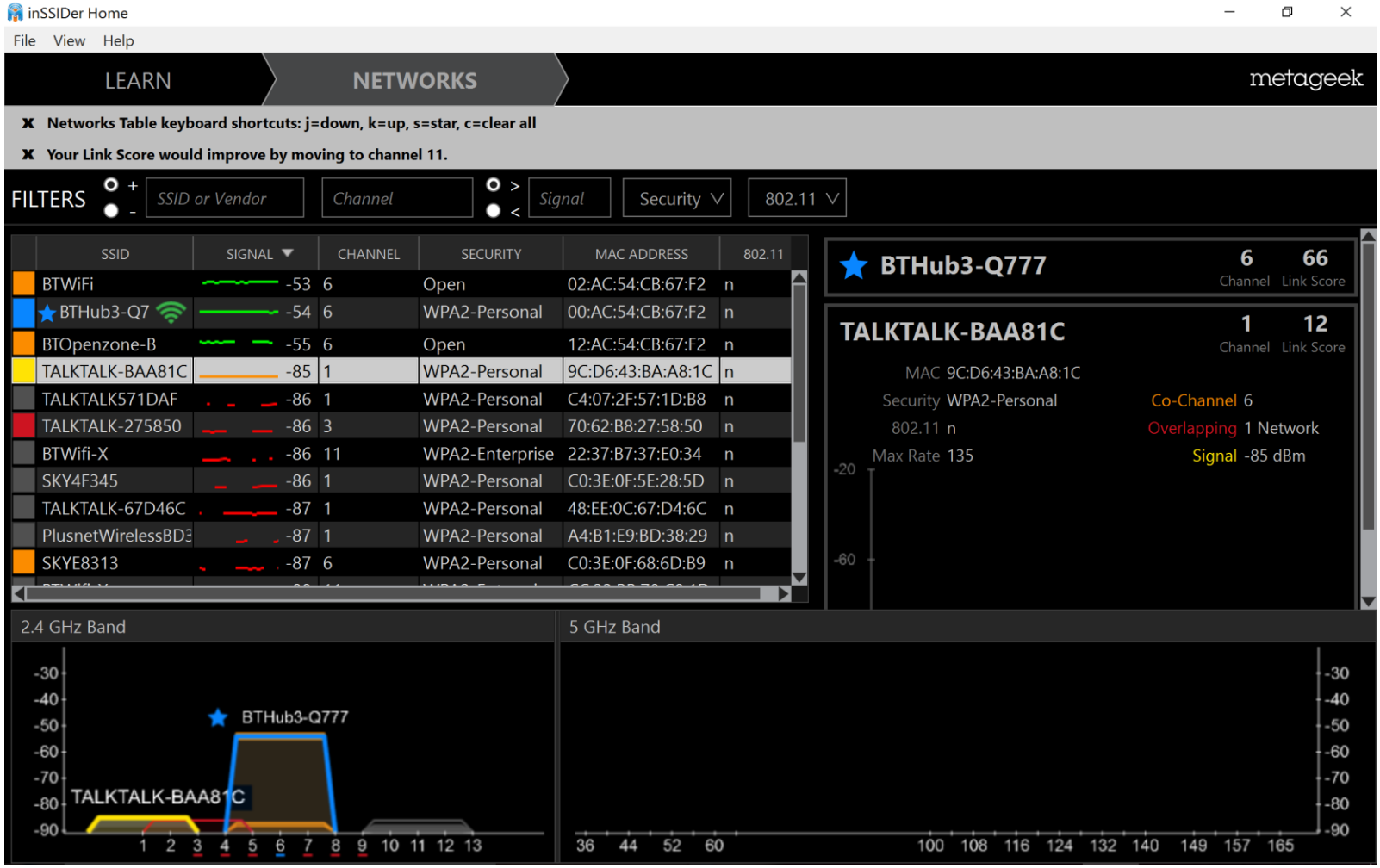
- Rogue AP
- Evil Twin
- WAR Driving
- Man in the Middle (MitM) Attacks
- Denial of Service (DOS)

WIRELESS SECURITY

- SSID Broadcast
- Default security settings
- MAC Filters
- Shielding
- Authentication
- Encryption



INSSIDER SOFTWARE



WIRELESS NETWORK SECURITY

The effective range of a wireless network is very difficult to predict, being dependant on such factors as obstacles, building materials, metal shielding, radiated power etc

A **site survey** is used to locate the optimum site for a new WAP or to conduct ongoing security checks.

- The transmitted power levels can be reduced on most access points to limit the range to within your boundary
- The type of antenna in use also affects how far wireless signals can travel, directional will travel further than omnidirectional
- Antenna placement should also avoid objects that interfere and be central so that coverage is overall

WIRELESS SURVEY (HEAT MAP)

Survey helps improve signal but also mitigate war driving

WIRELESS ANTENNAS

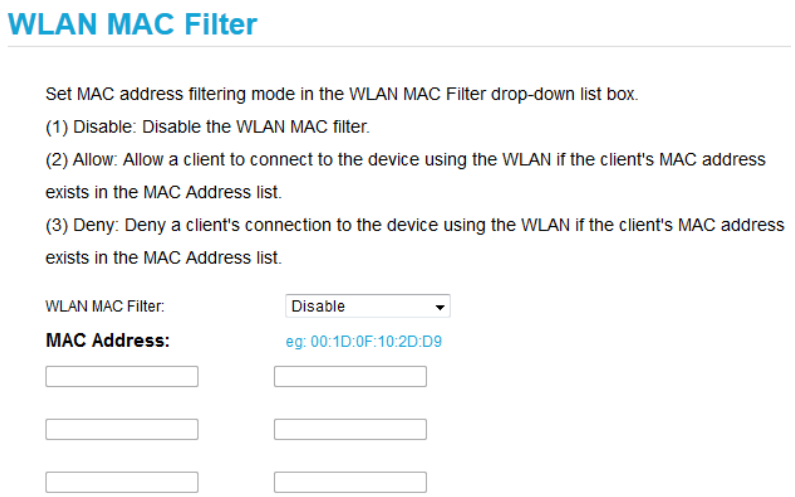
Transmit and Receive

Two Classes:

- Omni-directional (point to multipoint)
- Directional (Yagi, Cantenna, Panel, Parabolic) (point to point)

WIRELESS NETWORK SECURITY

- Mac Filtering – wireless networks can be made more secure by limiting the clients that are allowed to connect to the network
- This can be done by specifying the MAC addresses of the clients that can connect to the wireless network (whitelisting)
- This is configured on the wireless access point or router
- It is not fool proof because MAC addresses can be spoofed by the attacker for one of the allowed addresses



WIRELESS ENCRYPTION

WPA – Wi-Fi Protected Access replaced WEP and initially was more secure. Still in common use but now relatively easy to crack.

- Also uses RC4 encryption but this time with a 48 bit IV but uses TKIP as part of the encryption process
- TKIP – Temporal Key Integrity Protocol combines the IV with the key before encrypting and also changes the session key dynamically after a number of packets
- The weakness of WPA is the passphrase, a length of under 12 characters makes it breakable in a reasonable time

WIRELESS ENCRYPTION

WPA2 is the replacement for WPA and conforms to the 802.11i standard for security

- Uses the AES encryption algorithm along with CCMP
- Has been broken but is still seen as secure
- CCMP – Cipher block Chaining Message authentication Protocol is the process used with AES to provide encryption and provide confidentiality along with authentication of frames
- Personal & Enterprise. Personal uses a PSK and Enterprise some form of authentication system can be linked to SSO such as Kerberos.

WIRELESS ENCRYPTION

Wireless authentication can be handled by the access point or by an external server such as **RADIUS or TACACS+**

The standard that covers external authentication is **IEEE 802.1x**

There are other authentication mechanisms that are part of the EAP – Extensible Authentication Protocol framework. This allows for new technologies to be compatible with wireless. EAP is not usually encrypted

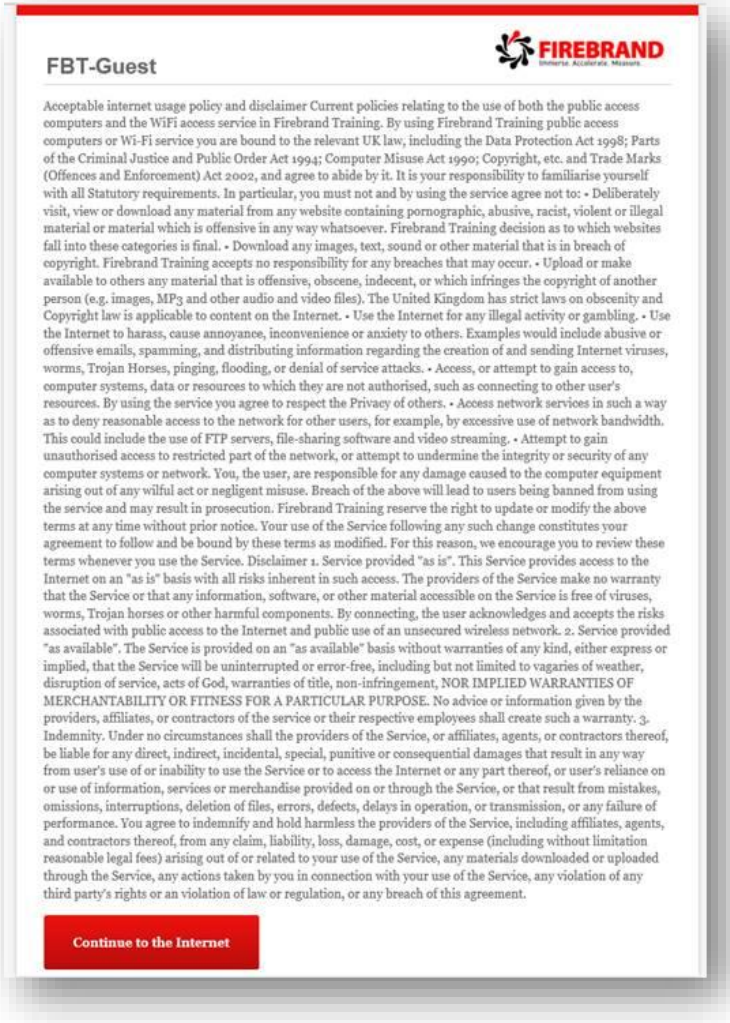
- **LEAP** – Lightweight EAP was developed by Cisco and was designed to replace TKIP in WPA
- **PEAP** – Protected EAP encapsulates EAP in a TLS tunnel which provides encryption

WIRELESS CONTROL

Captive Portals

Authentication technique used by companies to:

- Ensure logon credentials are used to access the WAP
- Request Payment for services
- Ensure Acceptable Use Policy / Health & Safety / Privacy Policies are read before gaining access



MODULE 11: AUTHENTICATION & ACCESS CONTROL

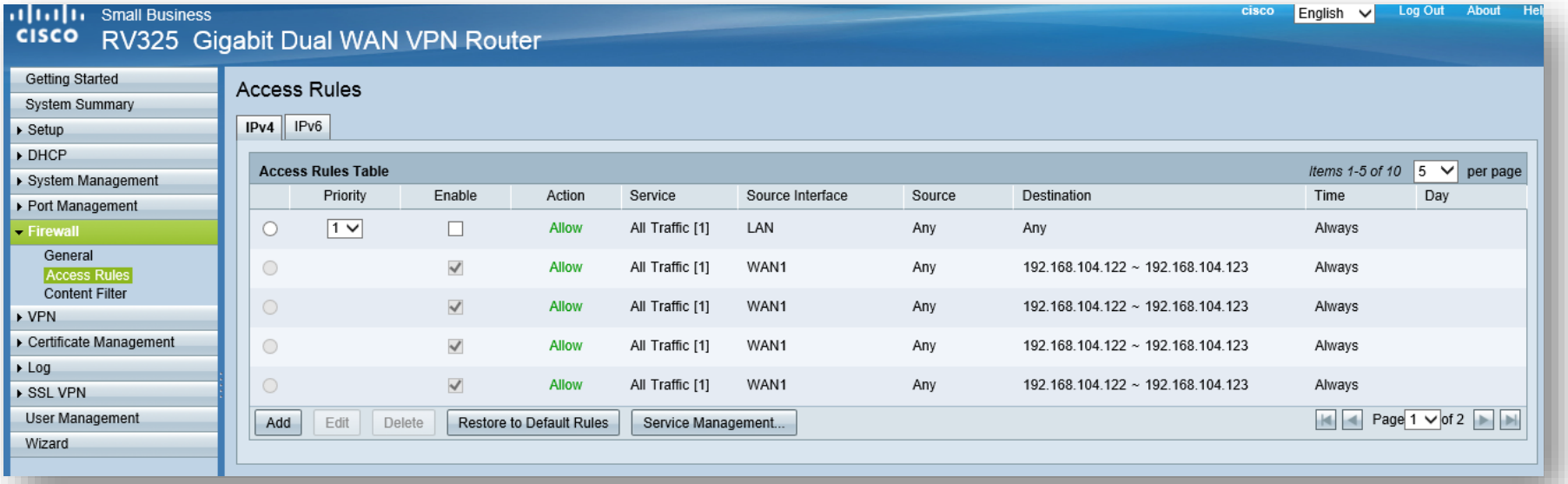
NETWORK+ 007

Your fastest way to learn. Guaranteed.

FIREBRAND

ACCESS CONTROL LIST (ACL)

Often ACLs are utilised on routers to determine which packets are allowed to route through, based on the requesting device's source or destination Internet Protocol (IP) address or Port Number (Port Filtering)



TUNNELING

Virtual Private Network (VPN)

Provides a secure connection between 2 endpoints using a variety of authentication and encryption techniques for the following:

- Remote Access (RAS) – Host-to-Site
- Site-to-Site / Host-to-Host
- Business-to-Business (B2) / Extranet VPN

VPN TYPES

The main types of tunnels to be familiar with:

- Secure Socket Layer (SSL)
- Layer 2 Tunneling Protocol (L2TP)
- Point to Point Tunneling Protocol (PPTP)
- IP Security (IPSEC)
- Generic Routing Encapsulation (GRE)

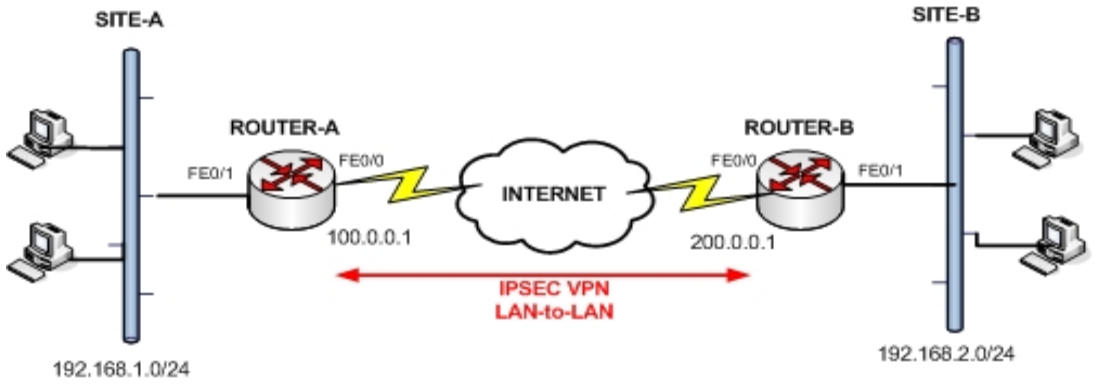
VPN TYPES

VPN	Port	Notes
PPTP	1723	
L2TP	1701	
IPSEC	500	ESP (id 50) / AH (id51)
GRE	47	
SSL	443	

IPSEC

Encapsulating Security Payload (ESP)
Authenticating Header (AH)
Security Association (ISAKMP)

- *Tunnel Mode*
- *Transport Mode*



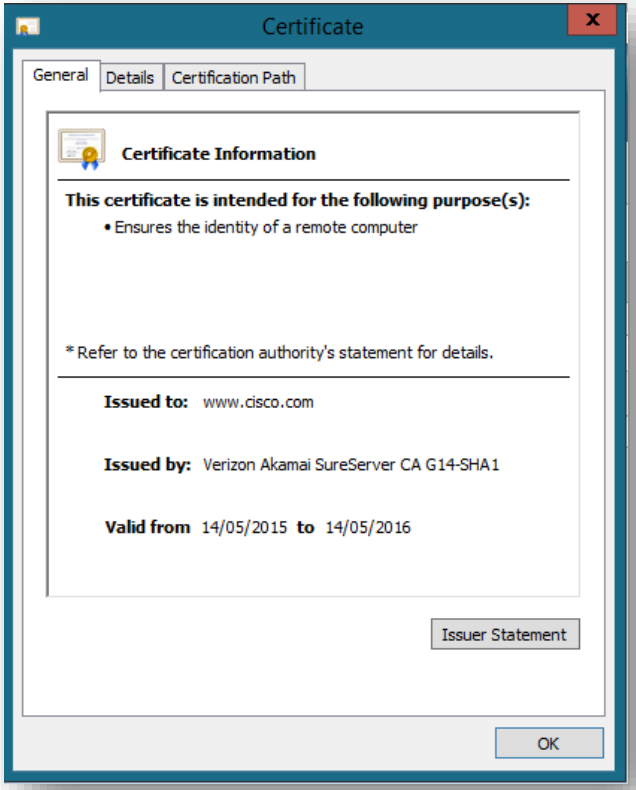
ENCRYPTION

SYMMETRIC

- DES
- 3DES
- AES

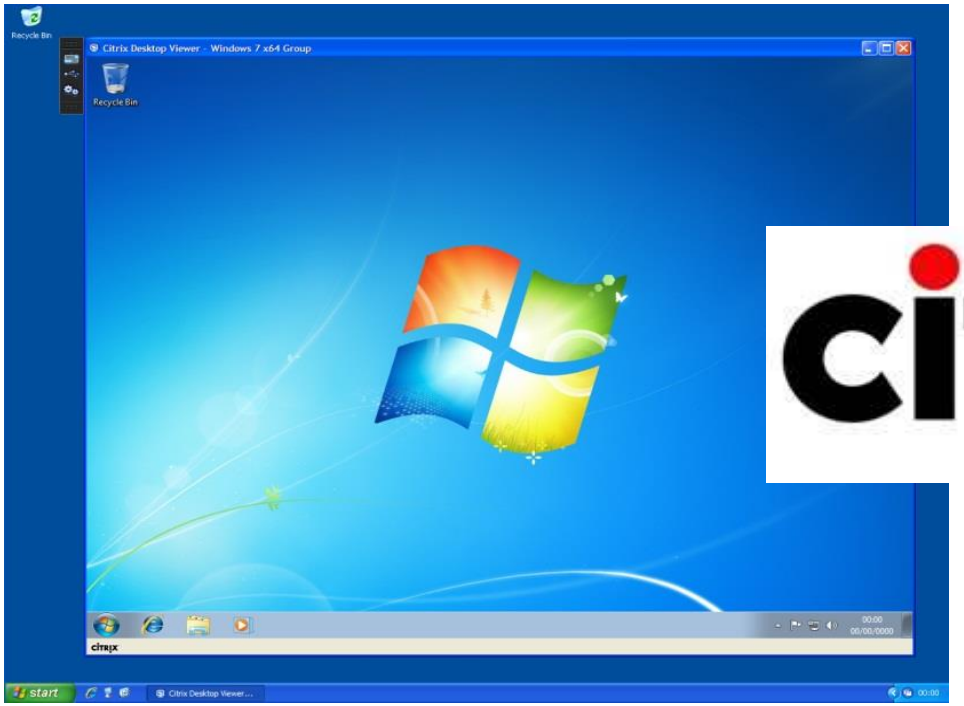
ASYMMETRIC

- PUBLIC & PRIVATE Key
- Diffie-Hellman
- RSA (Rivest, Shamir, Adleman)
- PGP (Pretty Good Privacy)



CITRIX

Terminal Emulation
Microsoft based Terminal Services on this technology



REMOTE DESKTOP

- Microsoft Remote Desktop Services / Terminal Services
- Uses Remote Desktop Protocol (RDP – Port 3389)
- May be secured with HTTPS
- Allows for Remote Desktops for Administration, Remote Assistance and Remote Applications
- May also be utilised in Virtual Desktop Infrastructure (VDI)

VDI

Virtual Desktop Infrastructure, or VDI, refers to the process of running a user desktop inside a virtual machine that lives on a server in the datacenter. It's a powerful form of desktop virtualization because it enables fully personalized desktops for each user with all the security and simplicity of centralized management.

Desktop virtualization is software technology that separates the desktop environment and associated application software device that is used to access it.

USER AUTHENTICATION

AUTHENTICATION – Proving you are who you say you are!

Authentication protocols:

- **Something that you know** – Password/Pin
- **Something that you have** – Smartcard/token
- **Something that you are -** Biometric

USER AUTHENTICATION

- Certificate Services (Public Key Infrastructure –PKI)
- Kerberos
- Active Directory (Domain)
- Local Authentication – Security Accounts Management (SAM)

AUTHENTICATION PROTOCOLS

- Password Authentication Protocol **PAP**
- Challenge Handshake Protocol **CHAP**
- Microsoft CHAP **MS-CHAP (MS-CHAPv2)**
- Extensible Authentication Protocol **EAP**
- **802.1x** – Network Access Control **NAC**

NETWORK ACCESS CONTROL

Cisco NAC / Microsoft NPAS (NAP)

Posture Assessment

- Antimalware
- Updates
- Firewall

Guest Networks

Quarantine Networks

AAA

Centralized **Authentication**, **Authorization** and **Accounting**:

Remote Authentication Dial-in User Service **RADIUS**

Terminal Access Controller Access-Controller System **TACACS+** (Cisco)

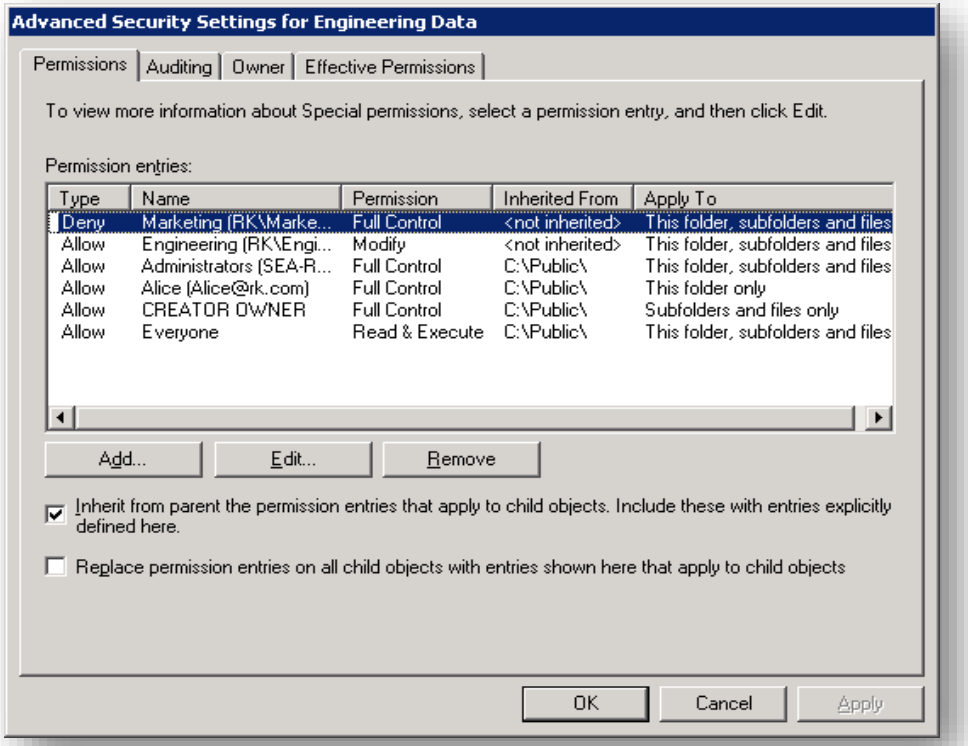
KERBEROS

Authentication protocol for TCP/IP networks allowing centralization of authentication on a single server (Domain Controller)

- Uses UDP / TCP port 88
- Key Distribution Center
- TGT (Ticket Granting Ticket)
- TGS (Ticket Granting Session)

AUTHORIZATION

- Permissions
- Rights
- Access Controls
- Share / Security Permissions
- Security Groups



MODULE 12: NETWORK THREATS

NETWORK+ 007

Your fastest way to learn. Guaranteed.

FIREBRAND

SECURITY

CIA

- Confidentiality
- Integrity
- Availability

AAA

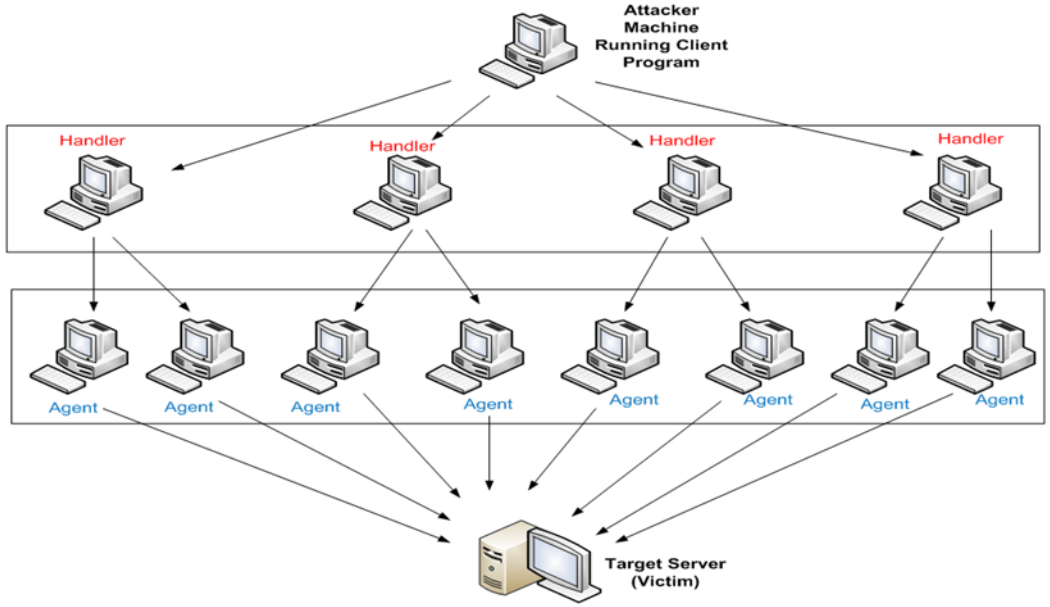
- Authentication
- Authorization
- Accounting

SECURITY THREATS

Denial of Service (DOS)

Distributed DOS (DDOS)

- Smurf
- Fraggle
- Botnet
- SYN Flood



SECURITY THREATS

- DNS Poisoning
- ARP Cache Poisoning
- IP Spoofing
- Session Hijacking
- VLAN Hopping

MALICIOUS SOFTWARE (MALWARE)

- Virus
- Worm
- Trojan Horse
- Rootkit
- Adware/Spyware

Antimalware / Antivirus

- System well patched and maintained

VULNERABILITIES

- Unnecessary Services/Applications
- Unpatched Systems/Applications
- Open Ports
- Unencrypted systems
- RF Emanation/TEMPEST
- Insider Threats

WIRELESS SECURITY

- WAR Driving / WAR Chalking
- WEP/WPA/WPA2 Cracking
- Rogue Access Point
- Evil Twin
- Bluejacking
- Bluesnarfing

SOCIAL ENGINEERING

- Using or manipulating users for nefarious gain – Flattery and Authority
- Phishing
- Vishing
- Tailgating
- Shoulder Surfing
- Hoax

SECURITY POLICIES

- Security Audit
- Clean Desk Policy
- Password Policy
- Acceptable Usage Policy

MITIGATION

User Training and Awareness

Patches and Upgrades

- OS
- Application
- Drivers
- Firmware

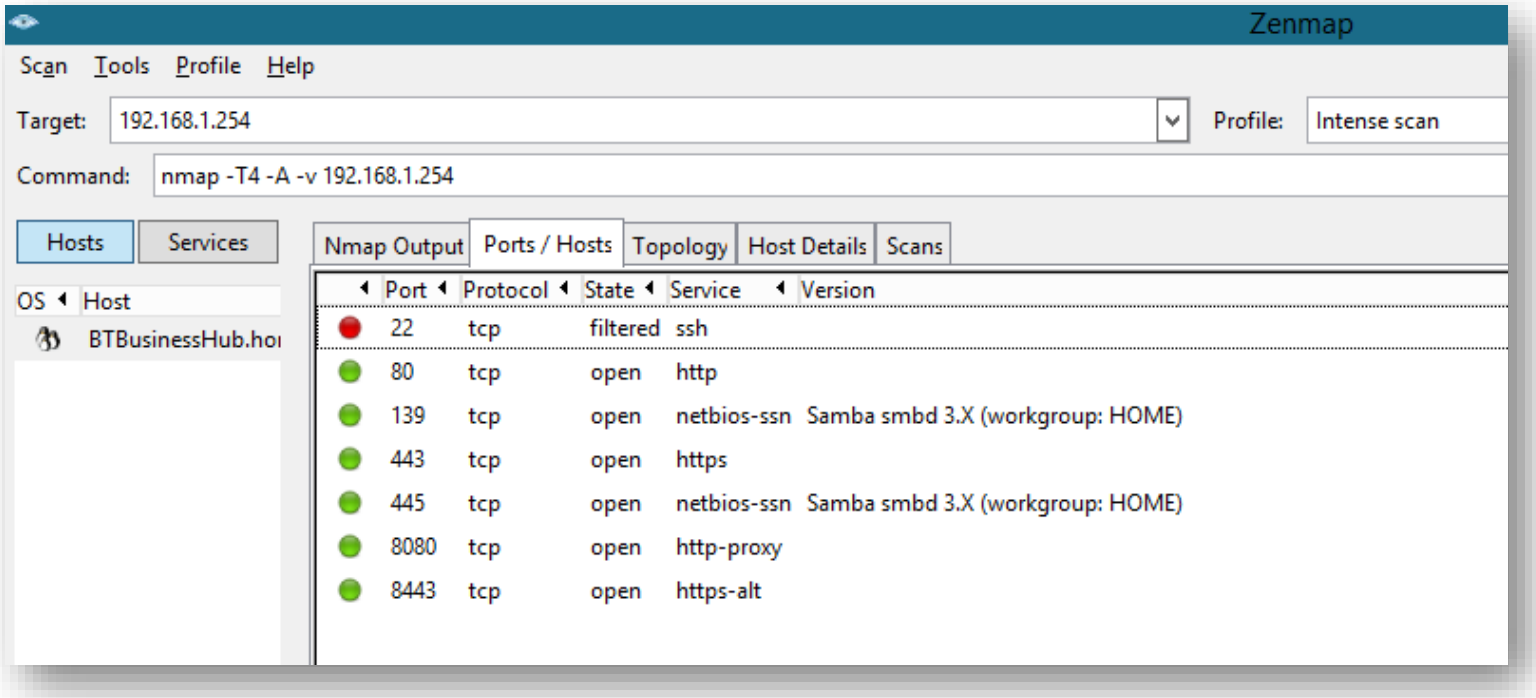
Anti-Malware Software

NETWORK SECURITY - MITIGATION

- Firewalls
- IDS
- IPS
- PROXY SERVERS

VULNERABILITY SCANNERS

NESSUS
NMAP
MBSA
OpenVAS



PHYSICAL SECURITY

- Security Zones
- Proximity readers
- Mantraps
- Badges/Tags
- Comms Room Security
- CCTV
- Access Controls

RISK AVOIDANCE

Disaster Recovery

- Disaster Recovery Plan (DRP)

Business Continuity

- Business Continuity Plan (BCP)

Power

- Redundant systems
- Uninterruptable Power Supply (UPS)

REDUNDANCY

DISKS

- RAID

POWER

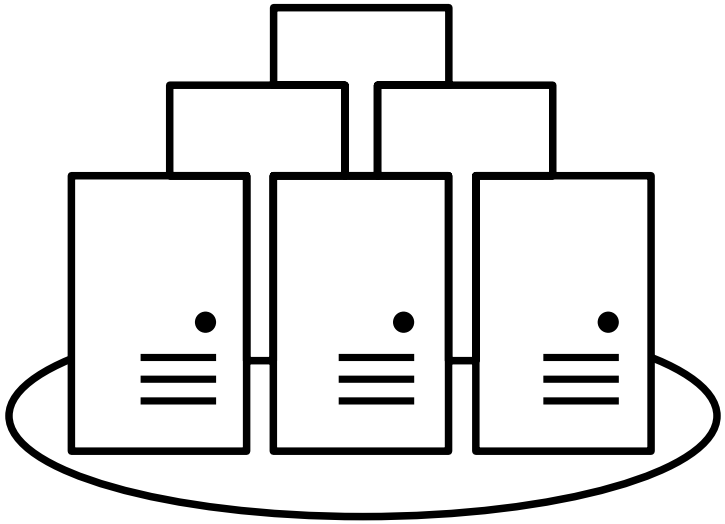
- UPS

SERVERS

- Clustering
- Virtualization

NETWORK

- Redundant Switches / NICs



RAID

RAID 0 - Stripping
RAID 1 - Mirroring
RAID 5 - Parity
RAID 10 – Stripe of Mirrors

MODULE 13: WIDE AREA NETWORKING

NETWORK+ 007

Your fastest way to learn. Guaranteed.

FIREBRAND

WAN MEDIA

Copper Carriers (Telephone Industry)

- T1 / T3 Lines

Fibre Carriers

- Synchronous Optical Network (SONET)(US)
- Synchronous Digital Hierarchy (SDH)(EUR)

COPPER CARRIERS

CARRIER	CHANNELS	SPEED
T1	24	1.544 Mbps
T3	672	44.736 Mbps
E1	32	2.048 Mbps
E3	512	34.368 Mbps

OPTICAL CARRIERS (SYNCHRONOUS OPTICAL NETWORK)

SONET Optical Level	Line Speed
OC-1	51.85 Mbps
OC-3	155.52 Mbps
OC-12	622.08 Mbps
OC-24	1.244 Gbps
OC-48	2.488 Gbps
OC-192	9.952 Gbps
OC-255	13.21 Gbps
OC-768	39.82 Gbps

FIBRE – WAVELENGTH DIVISION MULTIPLEXING

WDM – Allows for several different optical carriers on a single optical fibre by using different wavelengths.

Two technologies used are:

- DWDM – Dense WDM
- CWDM – Coarse WDM

PACKET SWITCHING

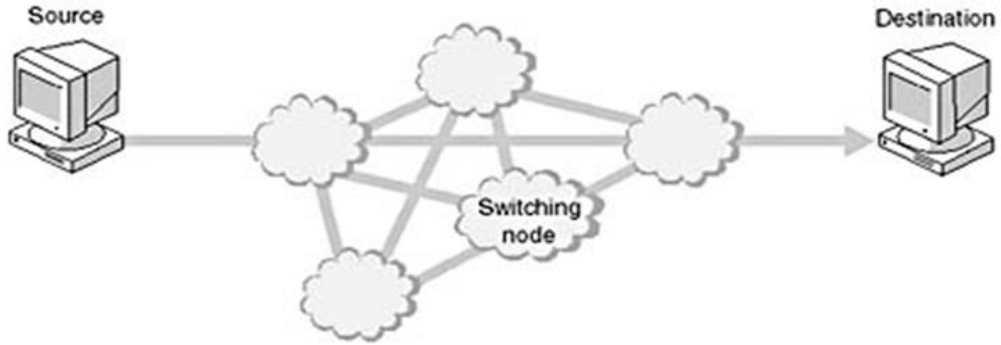
Allows for protocols to use T and OC linked mesh connections to ‘route’ from one location to another

Originally used X.25 (CCITT Packet Switching Protocol)

Now mostly uses:

Frame Relay

Asynchronous Transfer Mode (ATM)



FRAME RELAY

Primarily used for T-Carrier lines

Uses Frame Relay Bridges and/or Routers

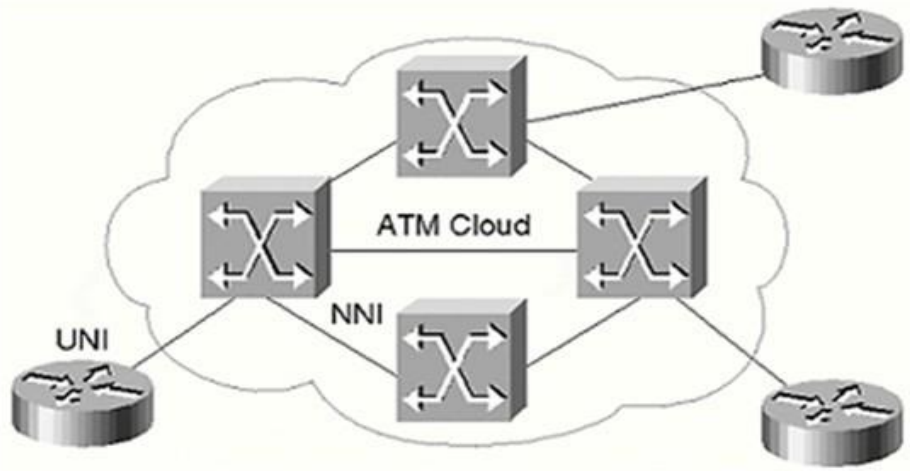
No guarantee of data integrity but low error rate

Creates a Permanent Virtual Circuit (PVC)

A permanent virtual circuit (PVC) is a virtual circuit established for repeated use between the same types of equipment.

ATM

- High speed reliable links used for:
- Voice
- Data
- Fax
- Media (Video/Audio/Imaging)



MULTI PROTOCOL LABEL SWITCHING (MPLS)

- Replacement for Frame Relay and ATM
- The process of transporting IP packets by encapsulating them and using a label to specify a path through the network
- The idea is based upon removing the need for routing table lookups
- Labels can be based upon source address, QoS value or other parameters
- Labels can override the routing table
- MPLS can run over a variety of layer 2 technologies

‘THE LAST MILE’

Connection between user and central office

- Dial-up
- Digital Subscriber Line (DSL)
- Cable
- Satellite
- Fibre
- Broadband over Powerline (BPL)

DIAL UP

- POTS or PSTN
- Expensive
- Unreliable
- Requires a dial-up
- Uses Point to Point Protocol (PPP) to connect, authenticate and negotiate network protocol *(TCP/IP)*

V-Standards

- *V.22 (1,200Bps) – V.92 (57,600 bps)*

INTEGRATED SERVICES DIGITAL NETWORK (ISDN)

ISDN consists of two Channels:

Bearer (B Channels)

Carry Data, Voice information

Delta (D Channels)

Carry setup and configuration information

Basic Rate Interface (BRI) uses 2B+D

Primary Rate Interface (PRI) uses 23B+D (US)

8-30B+D (EUR)

DSL

Asymmetric Digital Subscriber Line (ADSL)
Symmetric DSL (SDSL)
Very High Bitrate DSL (VDSL)

- Uses existing telephone lines via DSL modem
- Standard RJ11 connectors
- Low pass filters to remove DSL for telephone calls
- Always on

WIRELESS WAN

- Cellular WAN
- High Speed Packet Access (HSPA+)
- WiMAX (World Wide Interoperability for Microwave Access)
- LTE (Long Term Evolution)

VOIP

Uses existing IP network for voice calls

Uses three standards

- RTP – Real Time Transport Protocol
- SIP – Session Initiation Protocol
- H.323

TROUBLESHOOTING WAN ISSUES

Key problems areas:

- Lack of Internet connectivity
- Interface errors
- Split Horizon
- DNS
- Router configurations
- Security Policy (Firewalls)

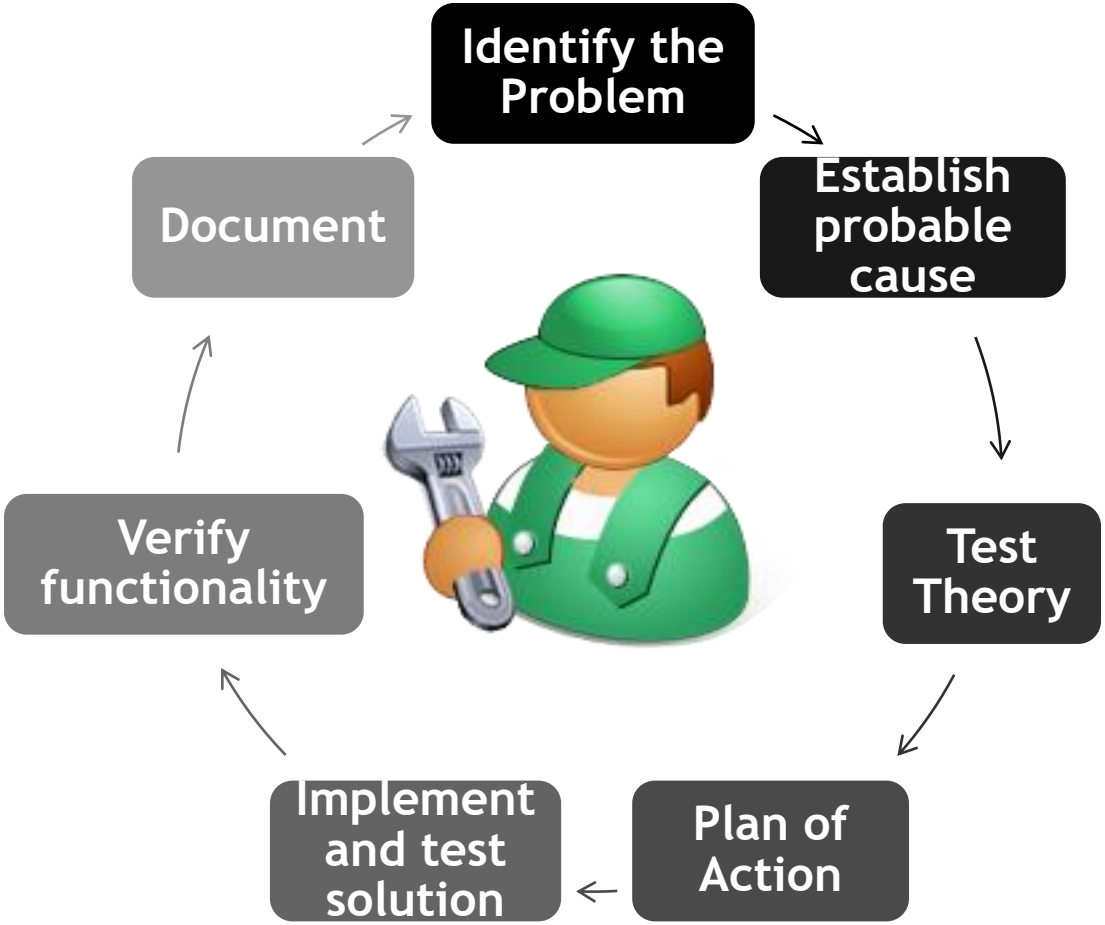
MODULE 14:TROUBLESHOOTING

NETWORK+ 007

Your fastest way to learn. Guaranteed.

FIREBRAND

BASICS OF TROUBLESHOOTING



TOOLS OF THE TRADE

- Protocol Analyzer
- Throughput Tester
- Remote Desktop Software
- Command Line Tools
- Wireless Analyzer

TCP/IP UTILITIES

IPCONFIG

/all

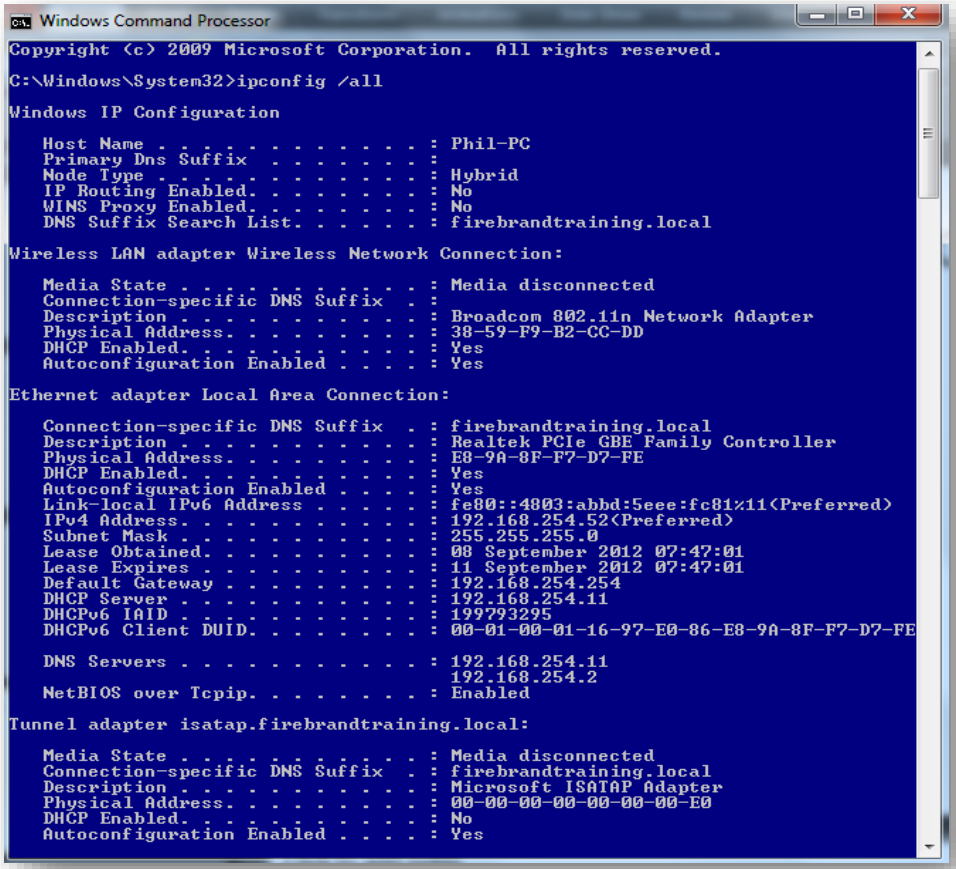
/displaydns

/registerdns

/flushdns

/release

/renew

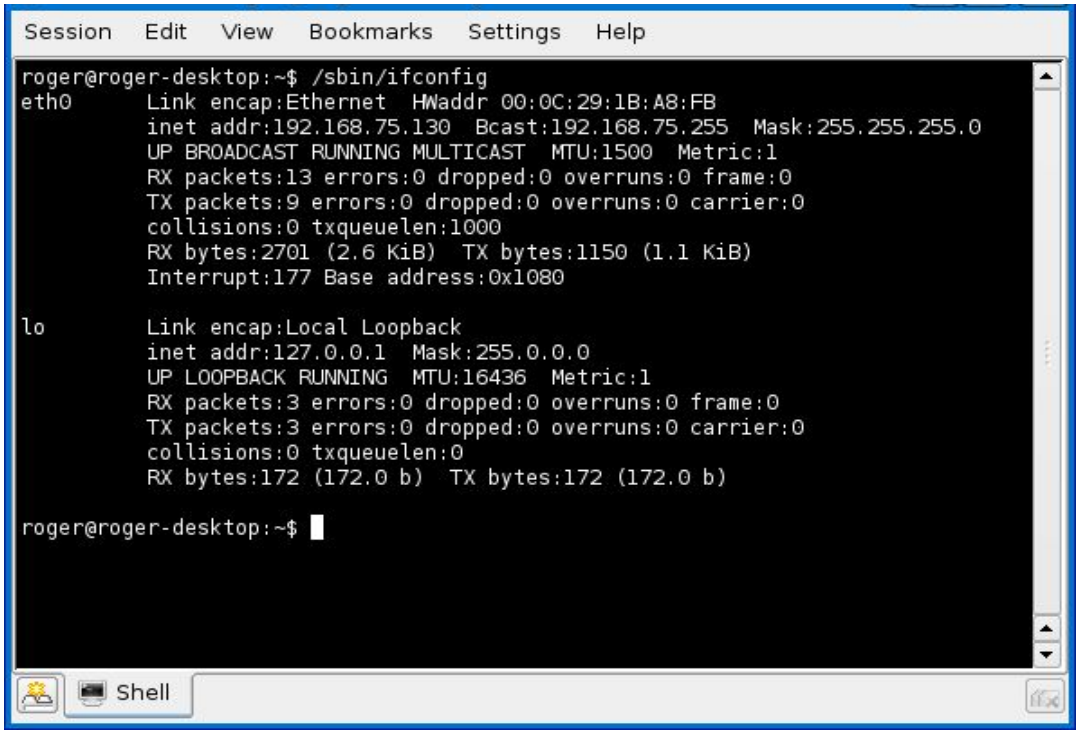


IPCONFIG

IFCONFIG (UNIX/LINUX)

Eth0 up (enables 1st Ethernet Card)

Eth0 down (disables)



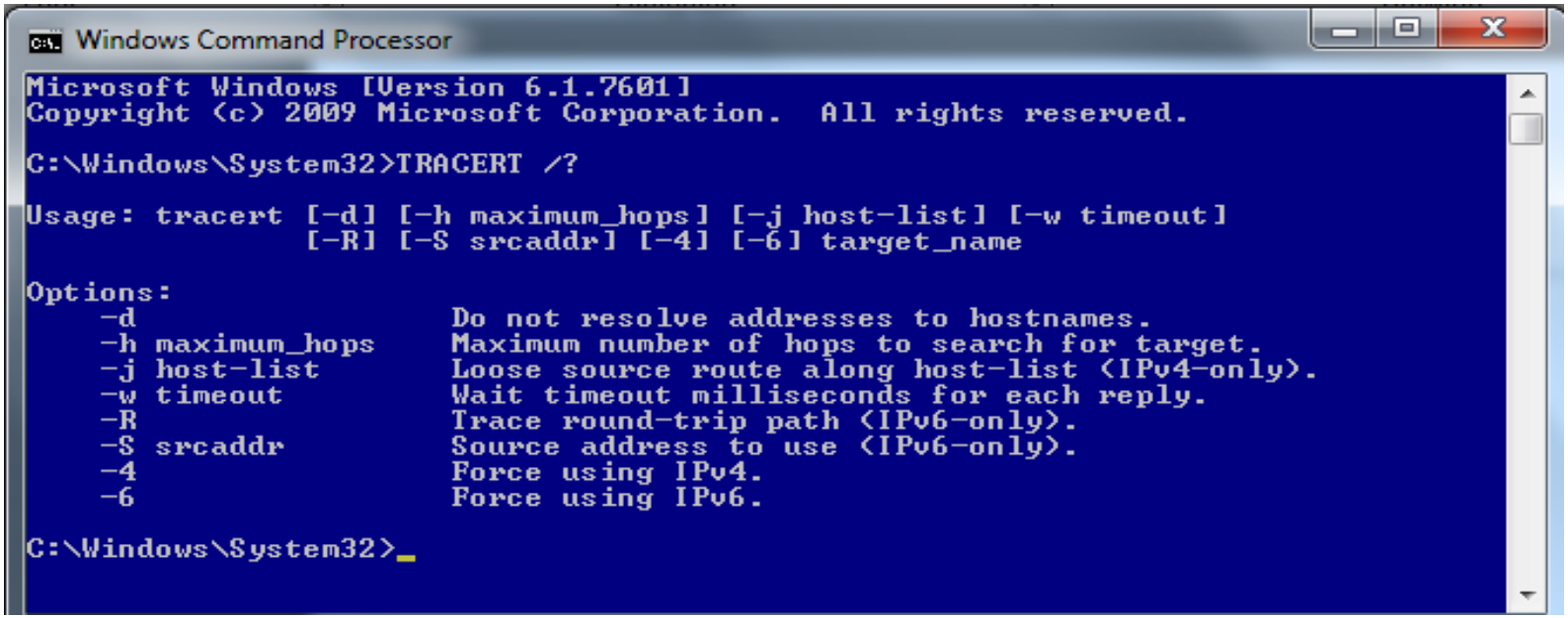
ICMP

PING

PATHPING

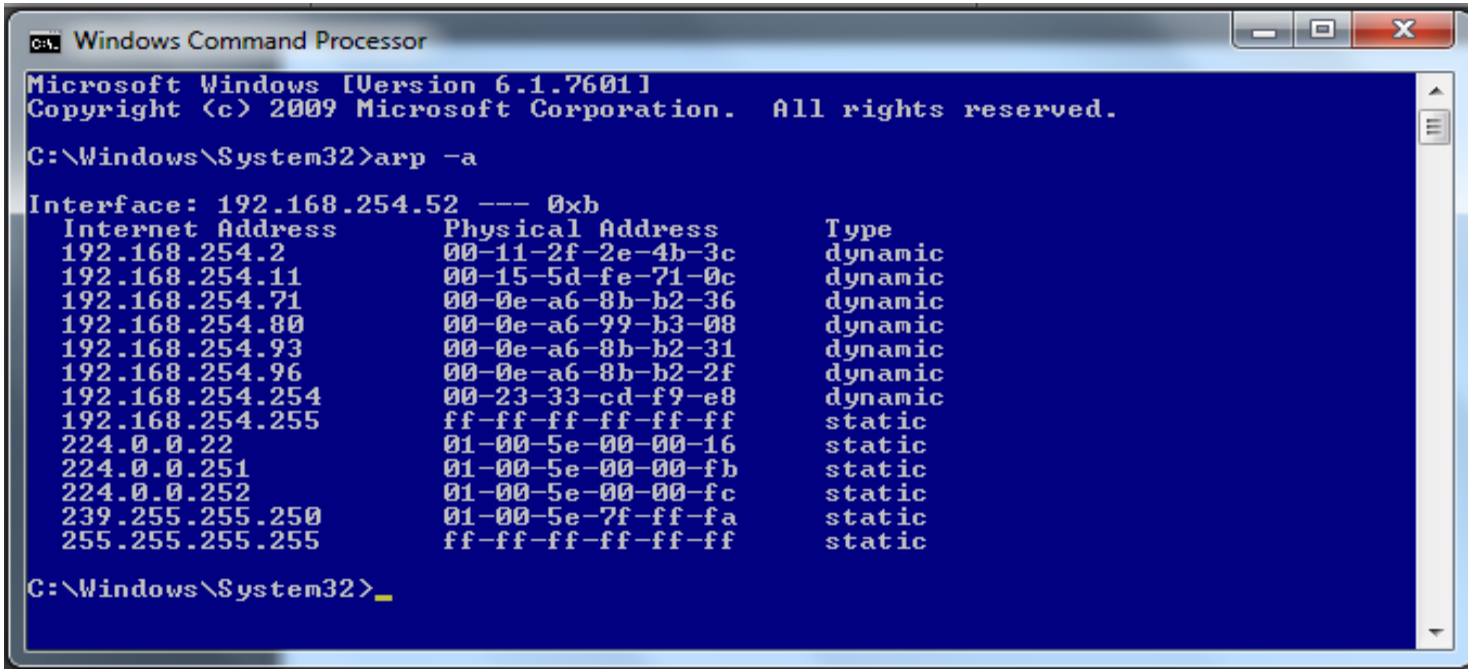
TRACERT

MTR (UNIX/LINUX) *(Similar to TRACERT and PING)*



ARP

Address Resolution Protocol
IP to MAC Address

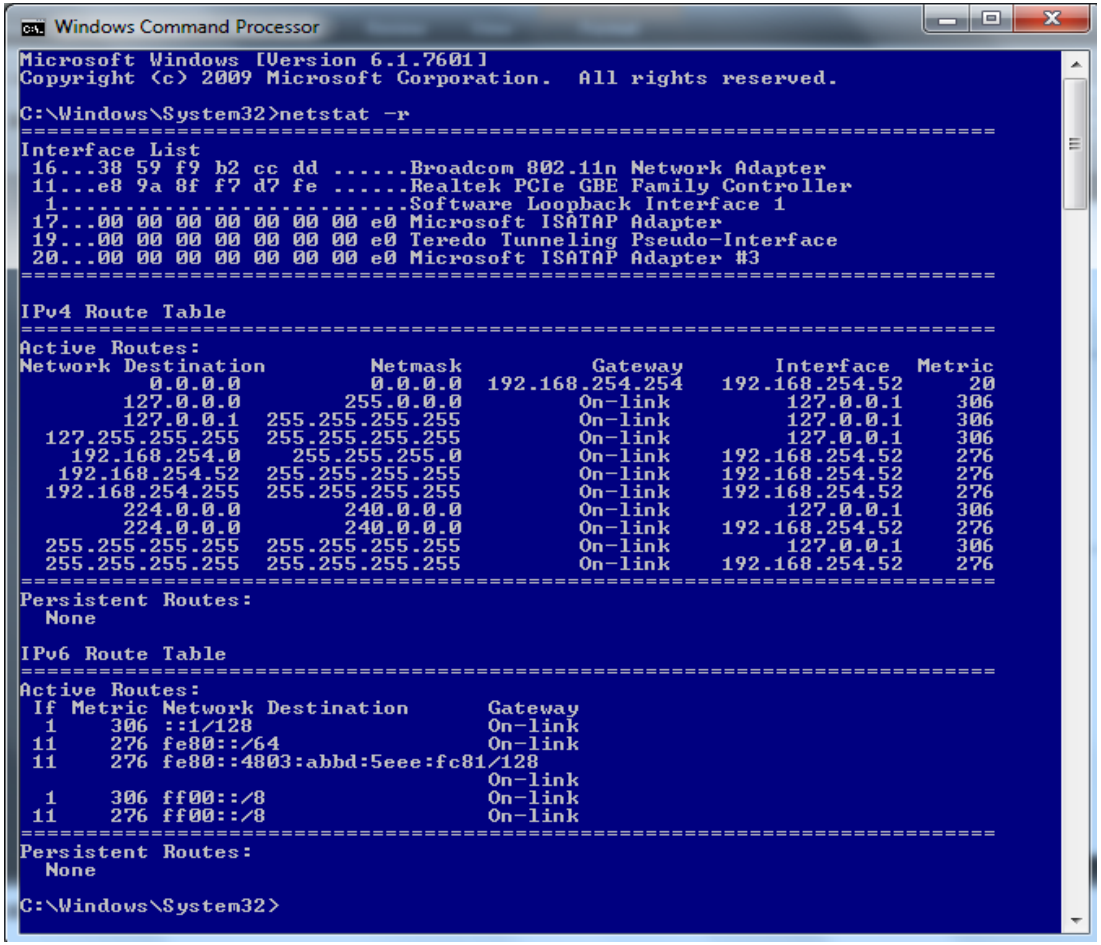


NETSTAT

-a (connections and listening ports)

-o (process ID)

-r (routing table)

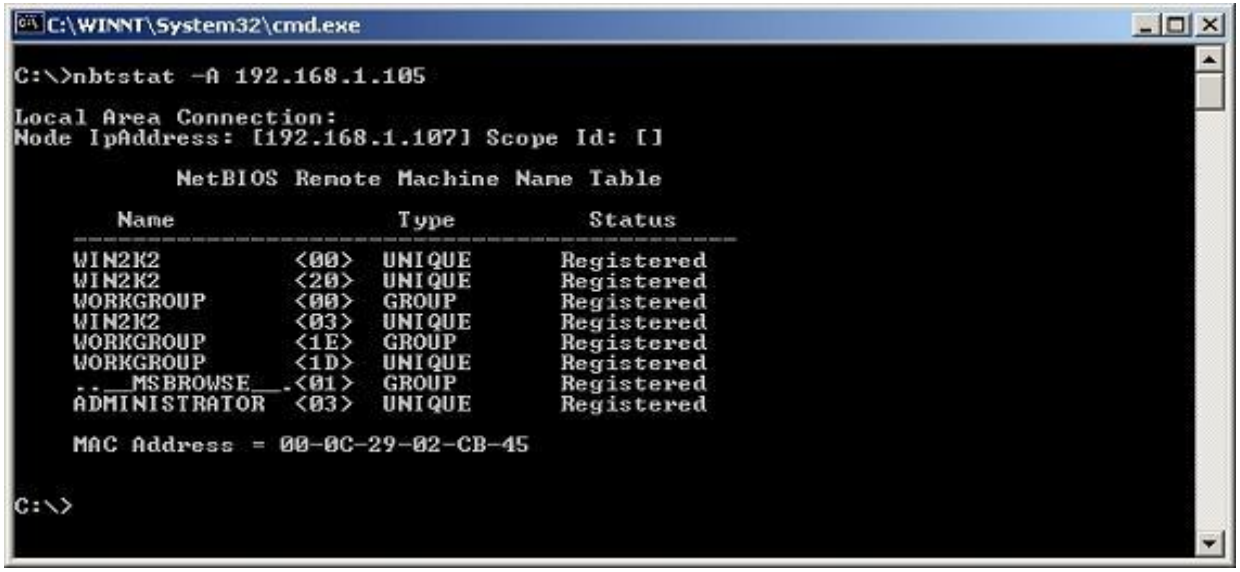


NBTSTAT

-n (local system)

-c (cache)

-R (purge and reload cache)



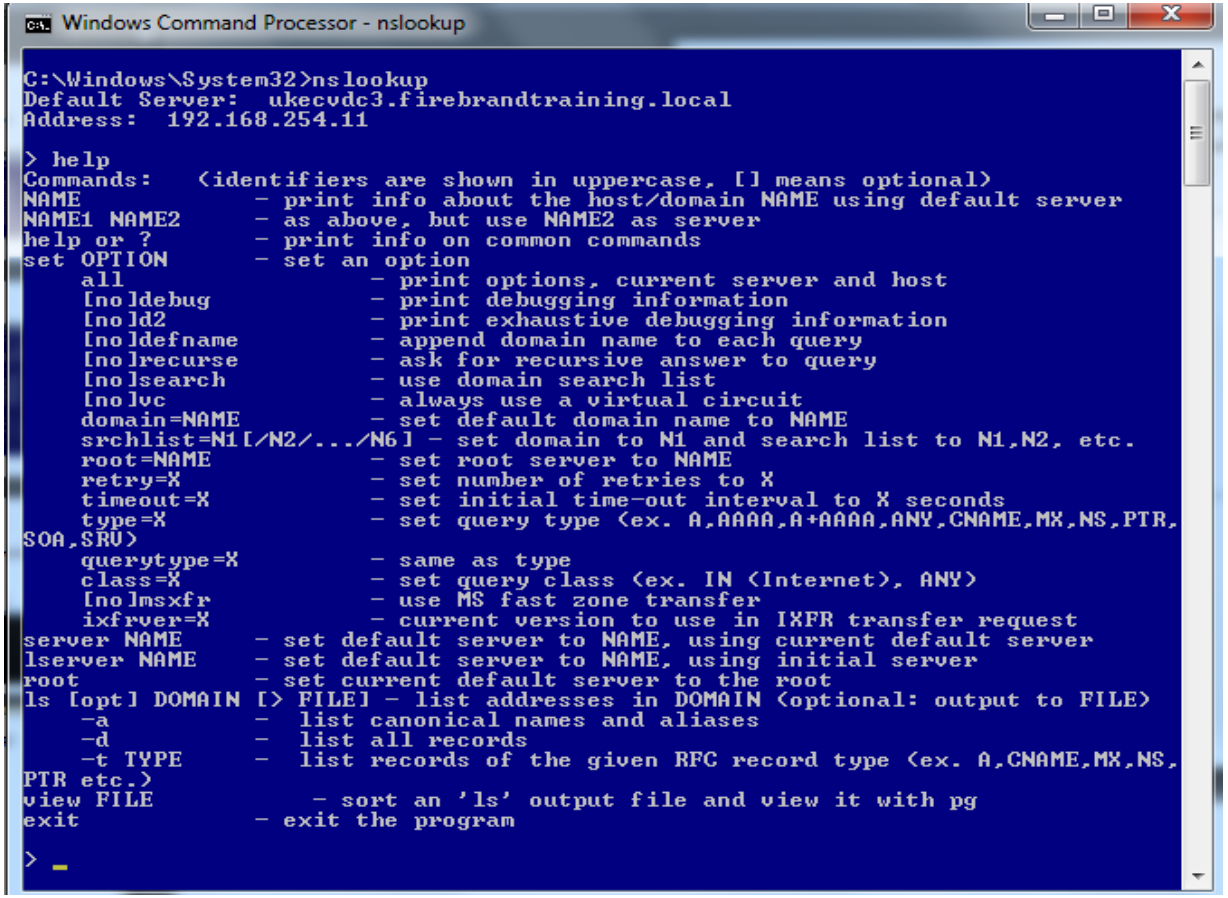
NSLOOKUP

DNS Diagnosis

-ls (list)

-d (domain)

-t (type)



DIG

UNIX/LINUX addition to NSLOOKUP

```
; <<>> DiG 9.7.2-P2 <<>> example.com -t ns
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51966
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;example.com.                   IN      NS

;; ANSWER SECTION:
example.com.            86400   IN      NS      a.iana-servers.net.
example.com.            86400   IN      NS      b.iana-servers.net.

;; Query time: 421 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Fri Oct 22 20:25:51 2010
;; MSG SIZE  rcvd: 77
```

NETWORK MONITORING

Baselines

- CPU
- RAM
- HDD
- NETWORK

Performance Monitor

System Logs (syslog)

Traffic Analyzer (Wireshark)

SNMP – Simple Network Management Protocol

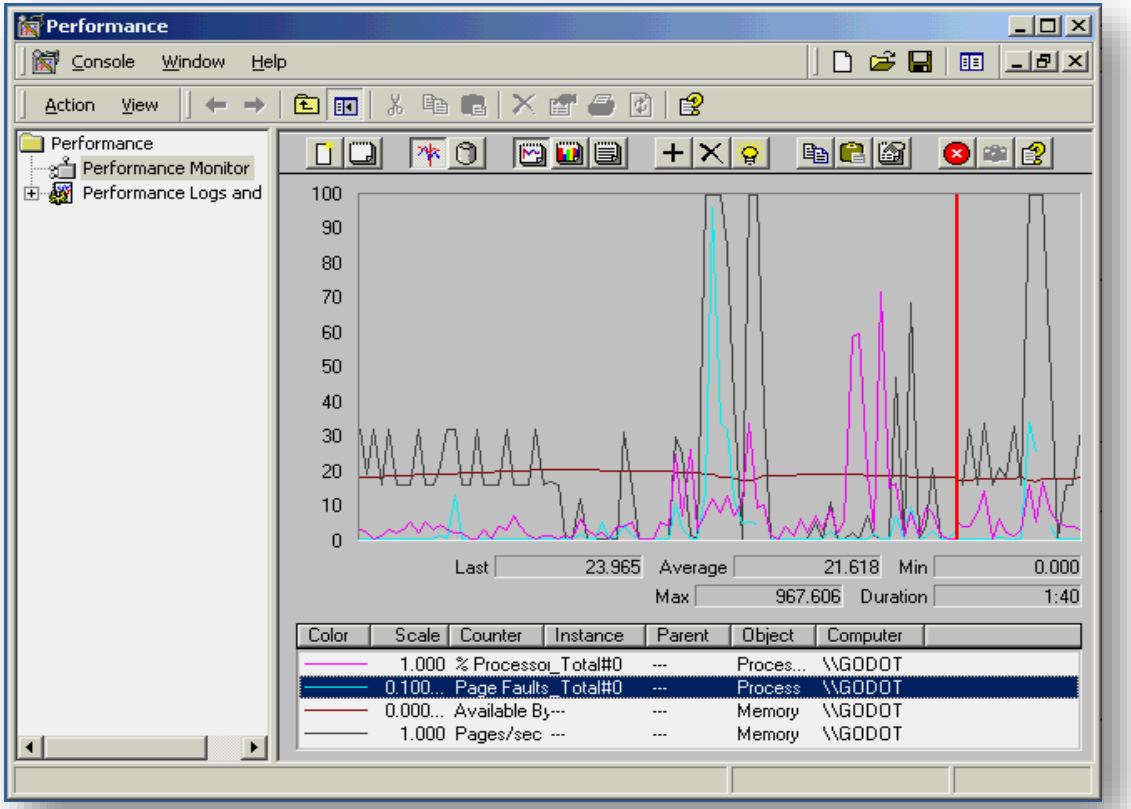
SIEM

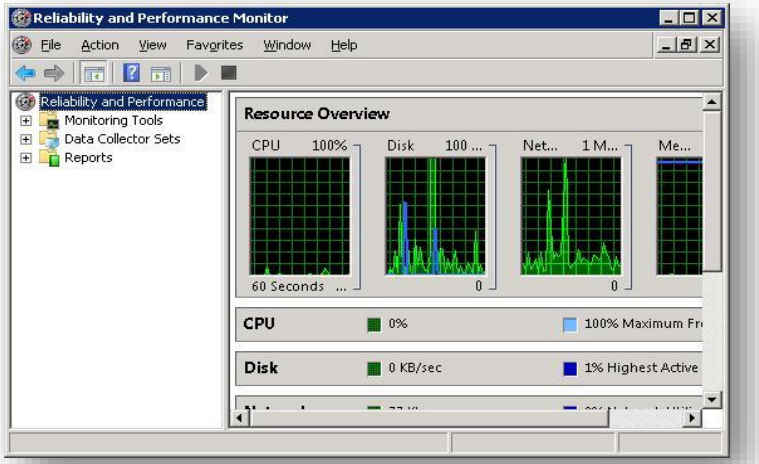
Security information and event management (SIEM) is a term for software products and services combining security information management

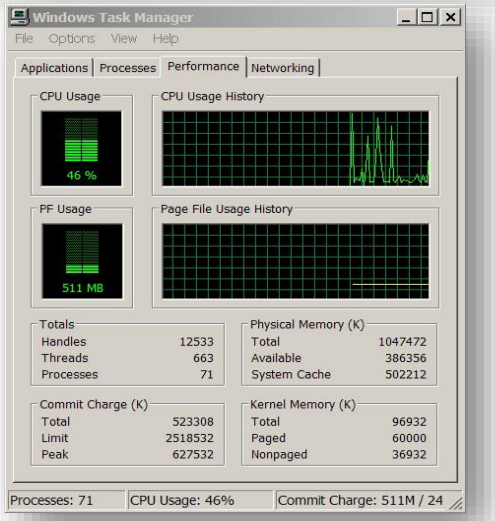
Used for the collation of the following types of information:

- **Data aggregation**
- **Correlation**
- **Alerting**
- **Compliance**
- **Retention**
- **Forensic analysis**

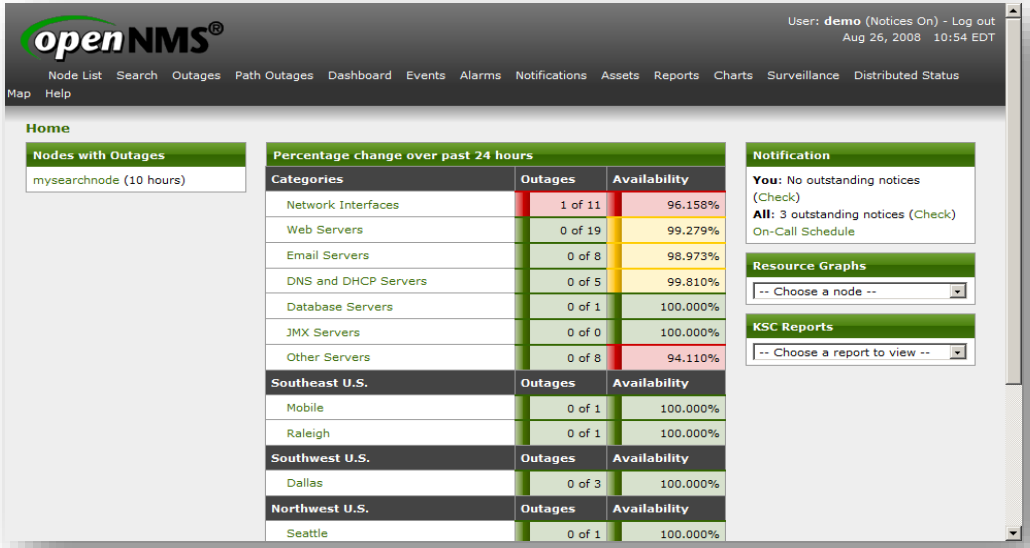
WINDOWS PERFORMANCE MONITORING

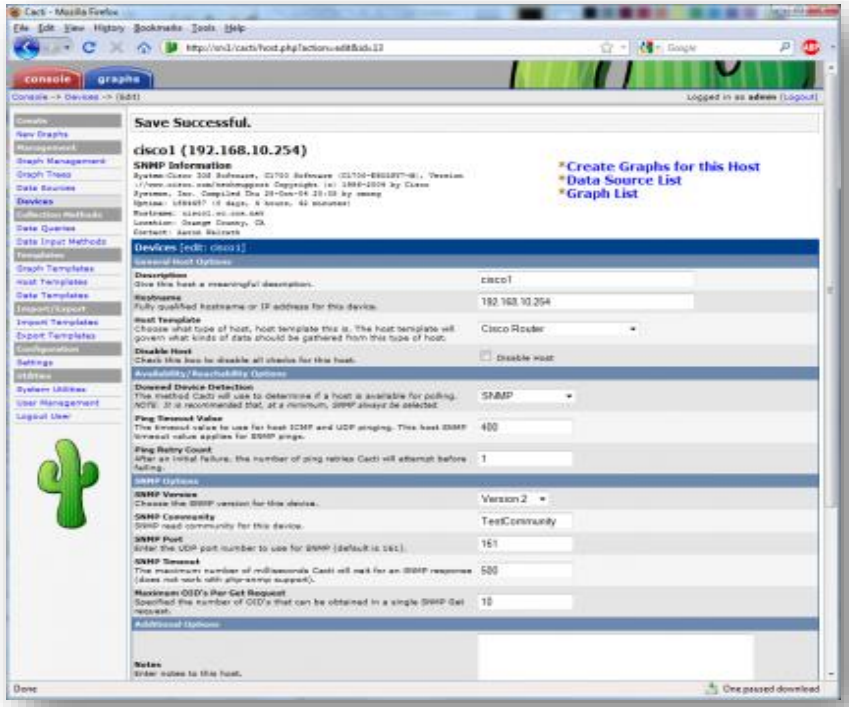






SNMP MONITORING





SIMPLE NETWORK MANAGEMENT PROTOCOL

- Allows the administrator to set a ‘trap’ on a device to collect information
- Uses UDP to send communication from the management system to the agent to get information or change configuration
- SNMPv3 adds message integrity, authentication and encryption.
- Uses port 161

TESTING EQUIPMENT

Multimeter

Testing resistance for shorts

TONE LOCATORS AND TONER PROBES

Locate cable runs

CABLE TESTER

- Broken wires
- Improperly wired
- Cable shorts
- May record speed and settings (Certifier)

CABLE TESTER (ADVANCED)

- Time-Domain Reflector (TDR)
- Optical TDR (for Fiber)

CABLE ISSUES

- Bad wiring/connectors
- Crosstalk
- Near End/Far End Crosstalk
- Attenuation
- Collisions
- Shorts
- Echo (Open Impedance Mismatch)
- Interference/EMI
- Split pairs
- TX/RX Reverse

FIBER CABLE ISSUES

- Cable Mismatch
- Bad connectors/dirty connectors
- Distance limitations
- Bend Radius

NETWORK ISSUES

- Web proxy failure – no internet access
- NIC failure – Cannot access network, APIA, look for lights, will loopback work - 127.0.0.1?
- Firewall – ACL, right order, blocked IPs, protocol, ports
- Switch failure – cannot access LAN
- Router Failure – cannot access parts of the network/WAN

CABLE STRIPPER / CRIMPER

BUTT SET

Used to test Telephone Lines

SYSTEM FAILURE

- Heat – check system fans, cooling, ventilation, HVAC, humidity.
- RAID – Check backplane, RAID battery
- Memory – Check it correctly seated, properly matched
- HDD/SSD – Replace as soon as it shows signs of failure when errors are reported, won't read or writ properly, bad clusters on HDD.
- CPU – CPU's fail usually when overloaded or heat, watch for intermittent system crash or system re-boots
- Power supply failure – system unresponsive 'no lights'
- Always check the physical elements first then work up the OSI model.

MODULE 15 MANAGEMENT, MONITORING & OPTIMISATION

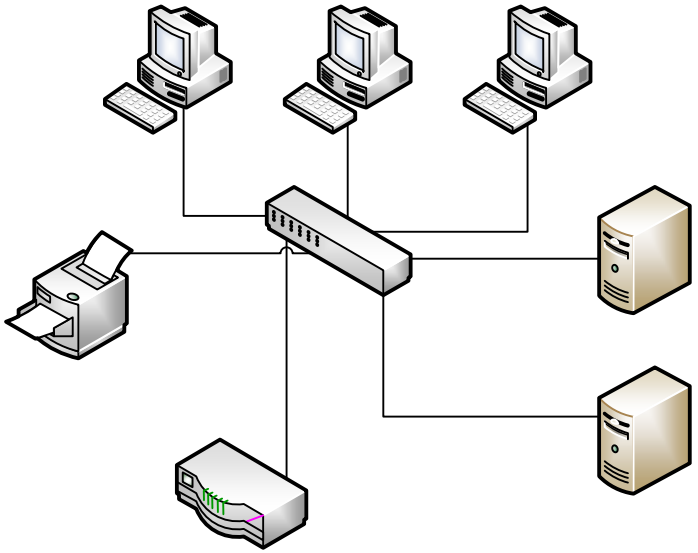
NETWORK+ 007

Your fastest way to learn. Guaranteed.

FIREBRAND

NETWORK MANAGEMENT

- Wiring Schematics
- Physical Network Diagram
- Physical Connections
- Network Devices
- Computers
- Peripherals



PHYSICAL DIAGRAM

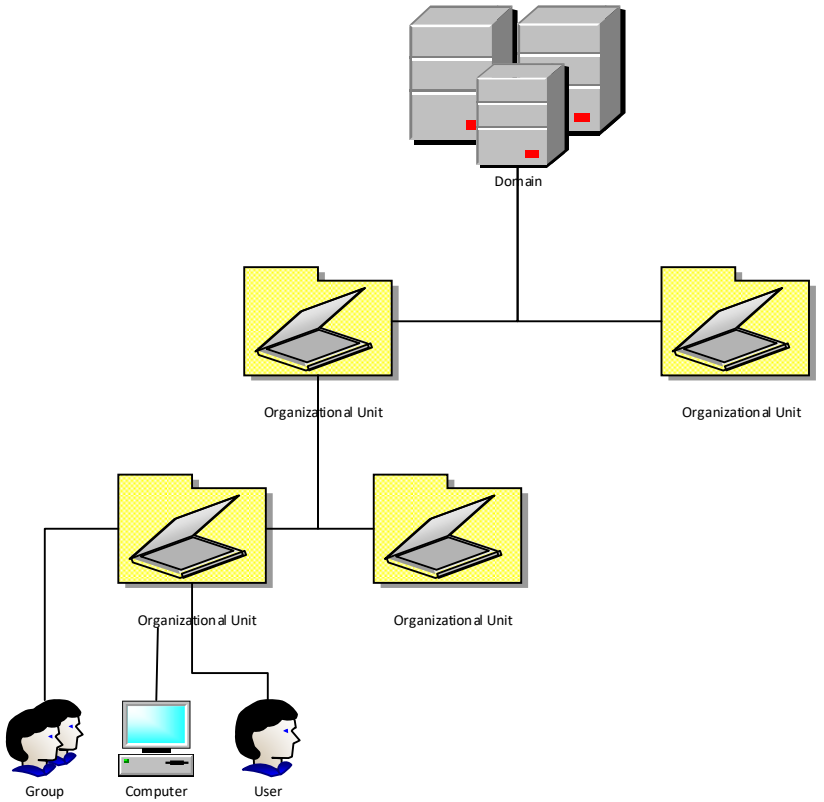
What happens if you have to rebuild your network from scratch?

Need a physical diagram all hardware and connections even current firmware versions, layout so you could replicate it should the worst happen.

NETWORK MANAGEMENT

Logical Network Diagram

- IP Address schemes
- Protocols
- User accounts



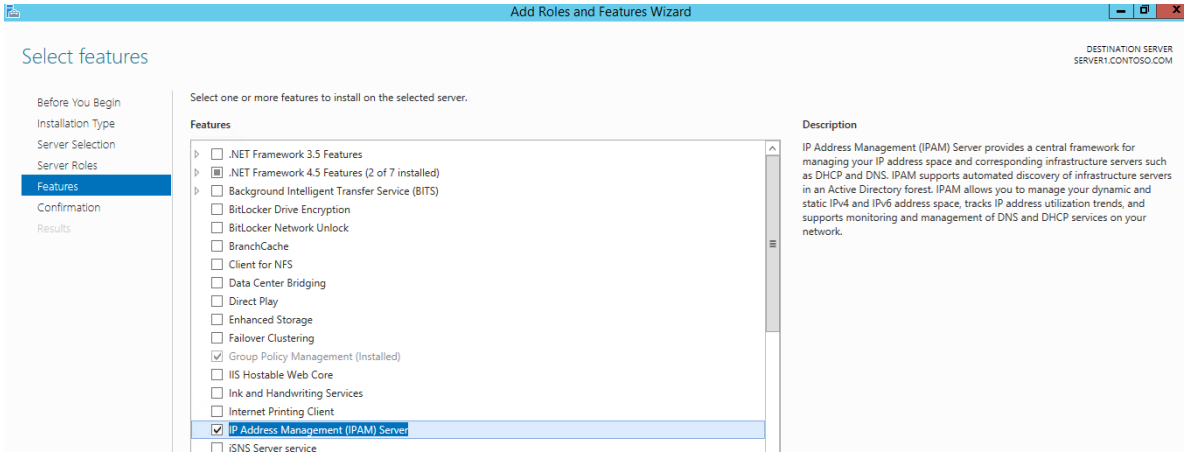
NETWORK MANAGEMENT

Asset Management

- ISO 19770

IP Address Management

- Documentation
- IPAM



NETWORK MANAGEMENT

Policies

- Security Policies
- Change Management

Standard Business Documents

- Statement of Work (SOW)
- Memorandum of Understanding (MOU)
- Master License Agreement (MLA)
- Service Level Agreement (SLA)

CHANGE MANAGEMENT PROCEDURES

- Document reason for change
- Change request
- Configuration procedures
- Rollback Process
- Potential Impact
- Notification

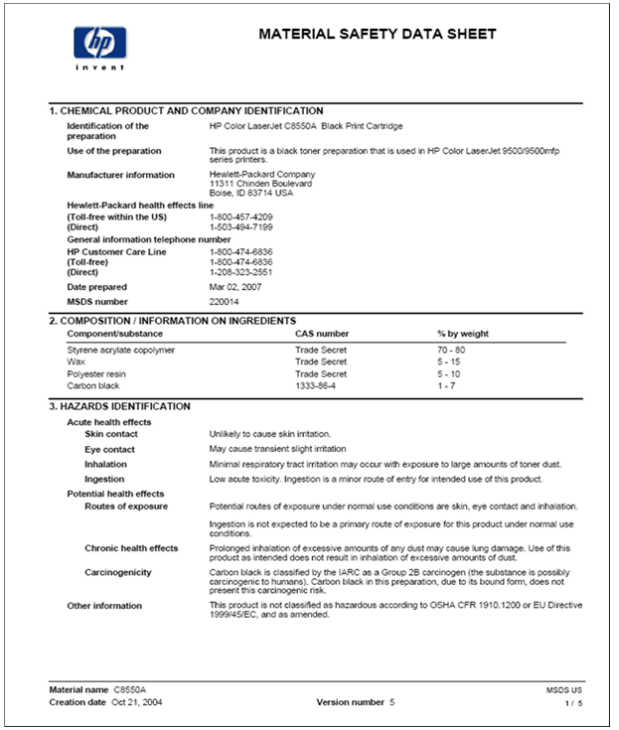
CHANGE MANAGEMENT PROCEDURES

- Approval Process
- Maintenance Window
- Authorized Downtime
- Notification of Change
- Documentation

NETWORK MANAGEMENT

Safety Practices

- Electrical Safety
- Installation Safety
- Material Safety Data Sheet (MSDS)



MATERIAL SAFETY DATA SHEET

1. CHEMICAL PRODUCT AND COMPANY IDENTIFICATION

Identification of the preparation	HP Color LaserJet C8550A Black Print Cartridge
Use of the preparation	This product is a black toner preparation that is used in HP Color LaserJet 9500/9500mfp series printers.
Manufacturer information	Hewlett-Packard Company 11311 Chinden Boulevard Boise, ID 83714 USA
Hewlett-Packard health effects line	
(Toll-free within the US)	1-800-457-4209
(Direct)	1-503-494-7199
General information telephone number	
HP Customer Care Line	1-800-474-6836
(Toll-free)	1-800-474-6836
(Direct)	1-208-323-2551
Date prepared	Mar 02, 2007
MSDS number	220014

2. COMPOSITION / INFORMATION ON INGREDIENTS

Component/substance	CAS number	% by weight
Styrene acrylate copolymer	Trade Secret	70 - 80
Wax	Trade Secret	5 - 15
Polyester resin	Trade Secret	5 - 10
Carbon black	1333-86-4	1 - 7

3. HAZARDS IDENTIFICATION

Acute health effects	
Skin contact	Unlikely to cause skin irritation.
Eye contact	May cause transient slight irritation
Inhalation	Minimal respiratory tract irritation may occur with exposure to large amounts of toner dust.
Ingestion	Low acute toxicity. Ingestion is a minor route of entry for intended use of this product.
Potential health effects	
Routes of exposure	Potential routes of exposure under normal use conditions are skin, eye contact and inhalation. Ingestion is not expected to be a primary route of exposure for this product under normal use conditions.
Chronic health effects	Prolonged inhalation of excessive amounts of any dust may cause lung damage. Use of this product as intended does not result in inhalation of excessive amounts of dust.
Carcinogenicity	Carbon black is classified by the IARC as a Group 2B carcinogen (the substance is possibly carcinogenic to humans). Carbon black in this preparation, due to its bound form, does not present this carcinogenic risk.
Other information	This product is not classified as hazardous according to OSHA CFR 1910.1200 or EU Directive 1999/45/EC, and as amended.

Material name C8550A MSDS US
Creation date Oct 21, 2004 **Version number** 5 1 / 5

NETWORK MANAGEMENT

Emergency Procedures

- Fire Escape Plan
- Safety/Emergency Exits
- Fail Open/Fail Close
- Emergency Alert System
- Fire Suppression System

NETWORK OPTIMIZATION

Performance

- QOS

Unified Communications

Bandwidth

- Traffic Shaping

Load Balancing

High Availability

Caching Engines

NETWORK OPTIMIZATION

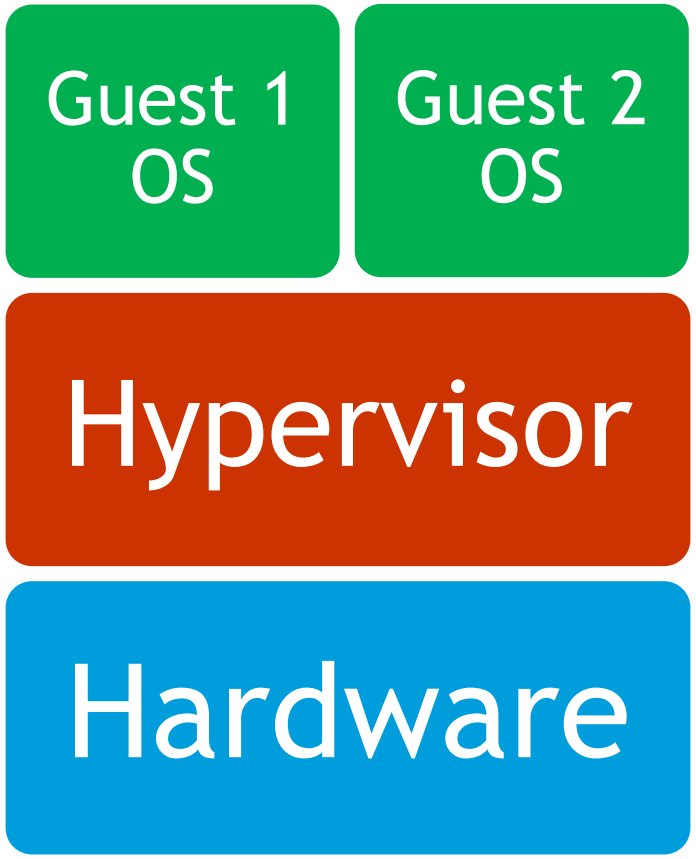
Backups

- Full
- Incremental
- Differential

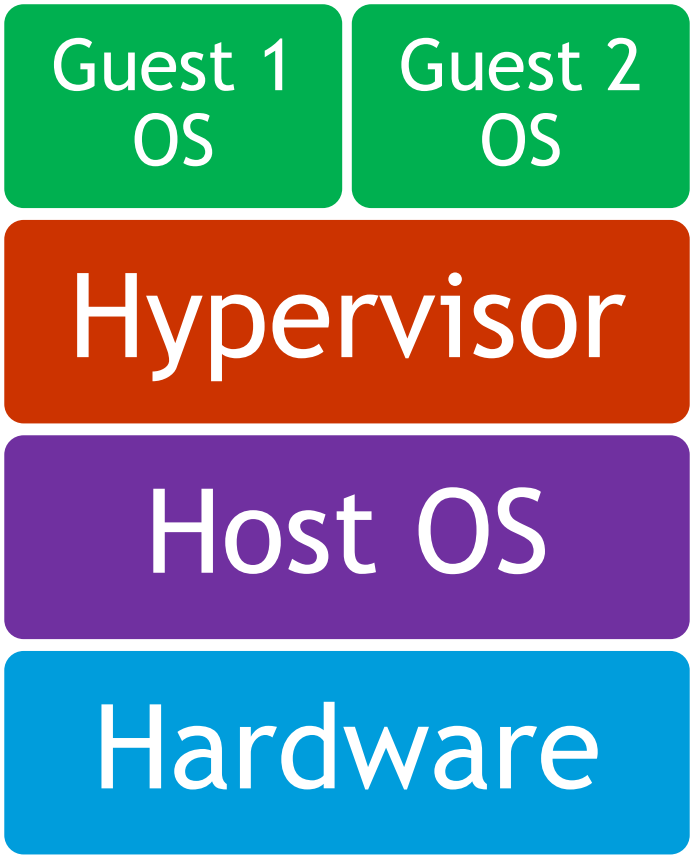
Backup Type	Data	Backup Time	Restore Time	Storage Space
FULL	All data	Slowest	Fastest	High
INCREMENTAL	New/Modified data	Fast	Slower	Low
DIFFERENTIAL	All data since last full	Moderate	Faster	Moderate

HYPERVISOR

Type I



Type II



VIRTUALIZATION

- Power Saving
- Consolidation of Hardware
- Recovery / Duplication
- Test and Development
- Costs

VIRTUALIZATION

- Virtual Networking (Switches)
- Virtual Hard Drives
- Virtual Desktops
- Virtual Applications
- Network/Infrastructure As A Service (NaaS)(IaaS)
- Platform As A Service (PaaS)
- Software As A Service (SaaS)

VIRTUALIZATION

Cloud Concepts

- Private
- Public
- Hybrid
- Community
- Elastic