MWR InfoSecurity

IBM Networking Attacks

. . . . Or the easiest way to own a mainframe without getting the removals men in

Martyn Ruks

2006-08-05

The harder way

On 27th September 2003 two men dressed as computer technicians arrived at Sydney International airport and succeeded in gaining access to the top-security computer room.

They disassembled two mainframe computers and walked out with them on trolleys.

The easier way

Much easier to use a laptop to get the information you need.

This is what will be discussed today !

Contents of the Talk

- Introduction
- Technical Background
- Attacking
- Recommendations

Introduction

Who am I ?

My name is Martyn Ruks and I am a Security Consultant with MWR InfoSecurity in the UK.

I have approached this subject from the perspective of a penetration tester and then as a security researcher. I do not have a background in IBM computing.

I believe that the investigation of IBM Networking security is made up of two parts: -

- Finding weaknesses that are known amongst administrators but aren't written down anywhere.
- Discovering vulnerabilities that are due to aspects of the technology that haven't been fully explored yet.

Intended Audience

This talk is aimed at the following people:

- Security Managers
- Penetration Testers
- Network and Security Architects
- Mainframe Operators

The only pre-requisite is an understanding of networking protocols and network architecture.

What is IBM Networking ?

My definition for the purpose of this presentation is as follows: -

A collection of protocols and networking technologies that allow IBM Mainframes, AS/400s and user terminals to communicate with each other.

The main protocol that we are going to be interested in is “Systems Network Architecture” (SNA).

“IBM Networking” also includes IP as it is a vital component of virtually all environments.

Why study IBM Networking?

The systems that communicate using it are usually business critical.

Aspects of it may be old but it is still used in a large number of high value environments.

It is always good to contrast protocols and compare vulnerabilities across technologies.

IBM networking technologies are never mentioned in security textbooks.

Technical Background

SNA – A brief history

SNA was first announced by IBM in 1974 and was intended to unify different IBM technologies.

It traditionally involved a master-slave model with input and output devices relying on the mainframe for everything.

All terminals, printers and other networking equipment must be configured on the mainframe. There wasn’t a concept of “plug and play” networking like there is today.

The architecture was designed with “secured” physical links in mind.

It was a time long before the widespread adoption of LAN technologies.

SNA – A brief history part 2

System to system networking was introduced with Advanced Peer-to-Peer Networking (APPN) in the 1980s.

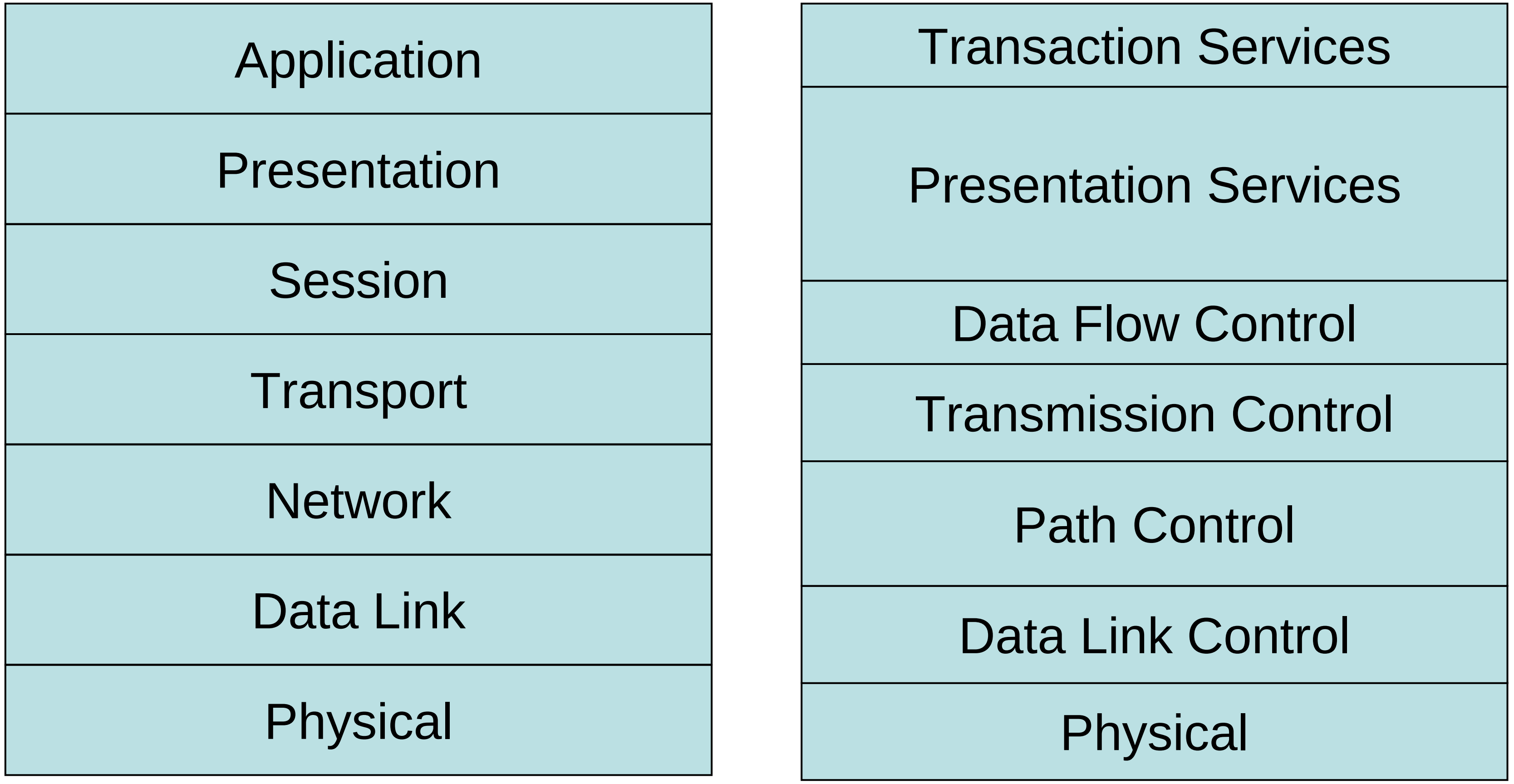
As the PC evolved, more responsibility was offloaded onto it from the traditional hardware.

There are now lots of different ways to enable IP and SNA to exist alongside each other.

The integration of old and new technologies is one reason that risk can be exposed.

Conceptual View of SNA

The SNA protocol approximately maps to the layers of the OSI model.



Application

Presentation

Session

Transport

Network

Data Link

Physical

OSI

Transaction Services

Presentation Services

Data Flow Control

Transmission Control

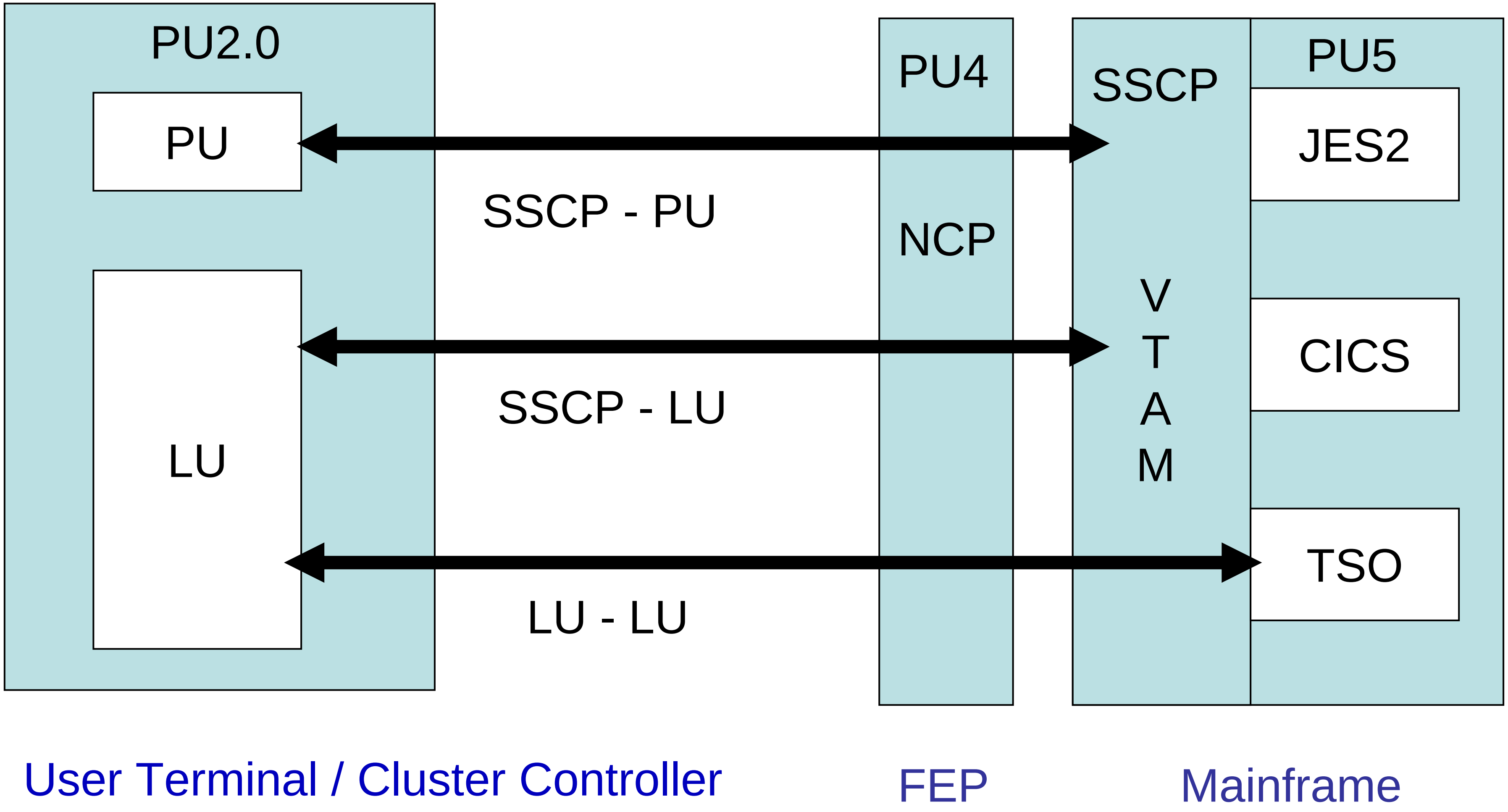
Path Control

Data Link Control

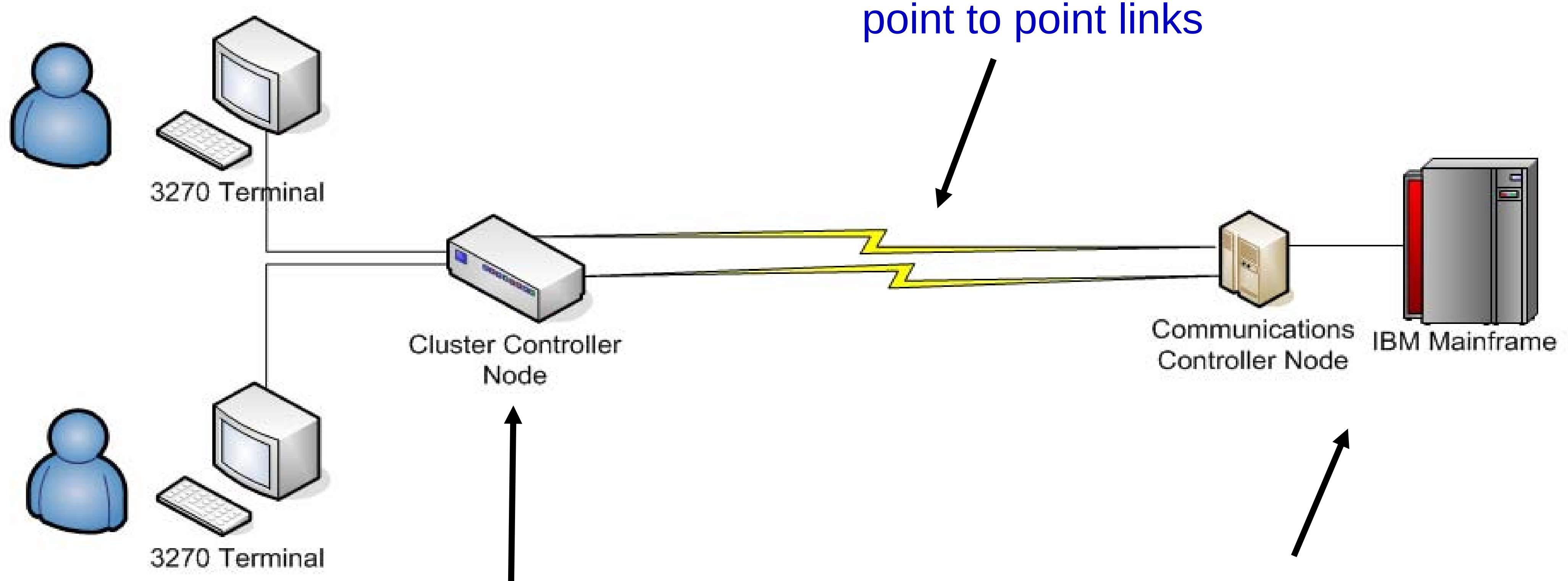
Physical

SNA

Different Sessions



Example 1: Basic SNA Network

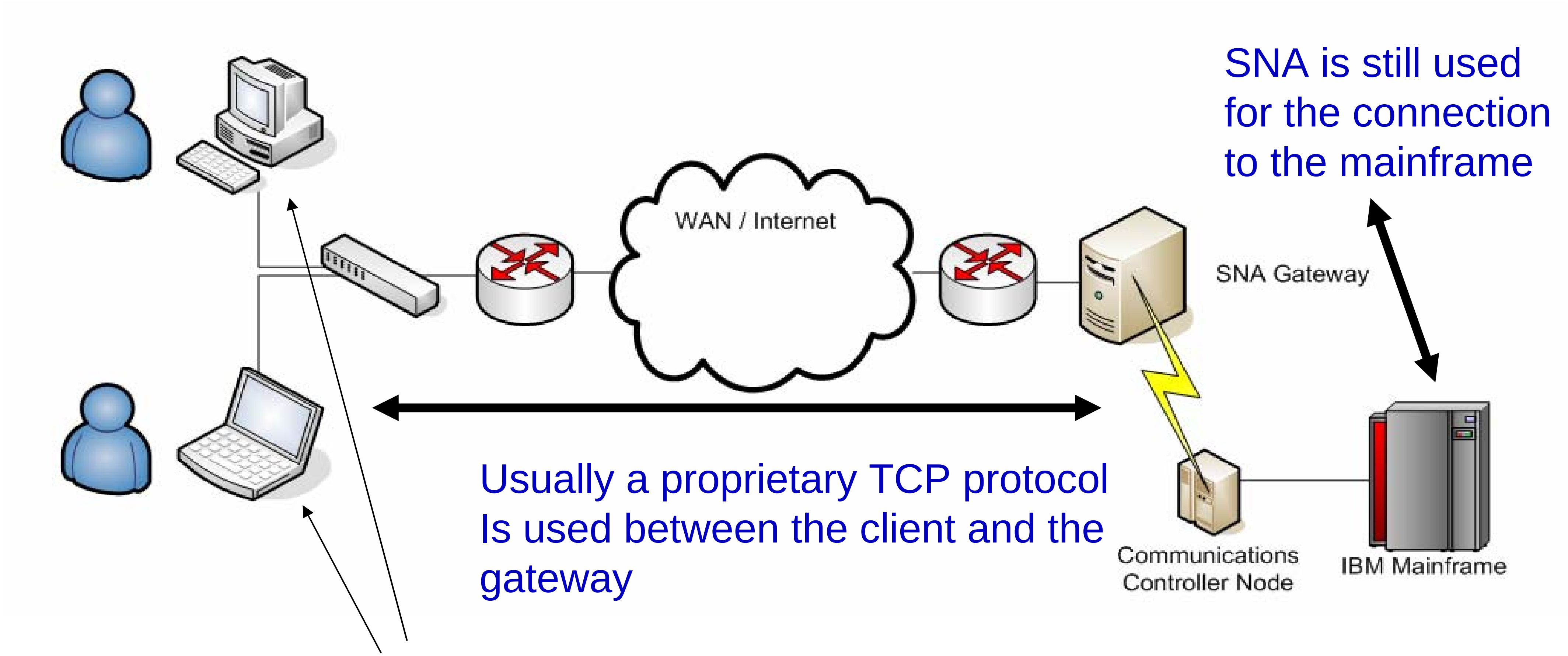


Fixed line SDLC point to point links

All terminals are physically connected to the Controller

All nodes must be defined within VTAM on the Mainframe

Example 2 – SNA Gateway



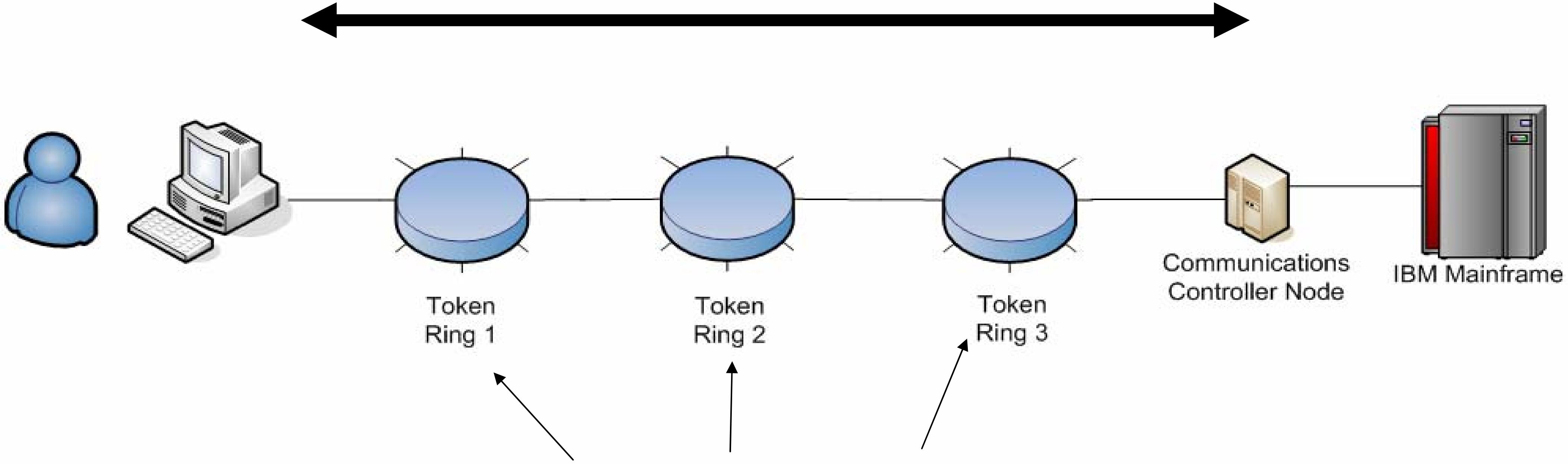
SNA is still used for the connection to the mainframe

Usually a proprietary TCP protocol Is used between the client and the gateway

Users running gateway server's client access application

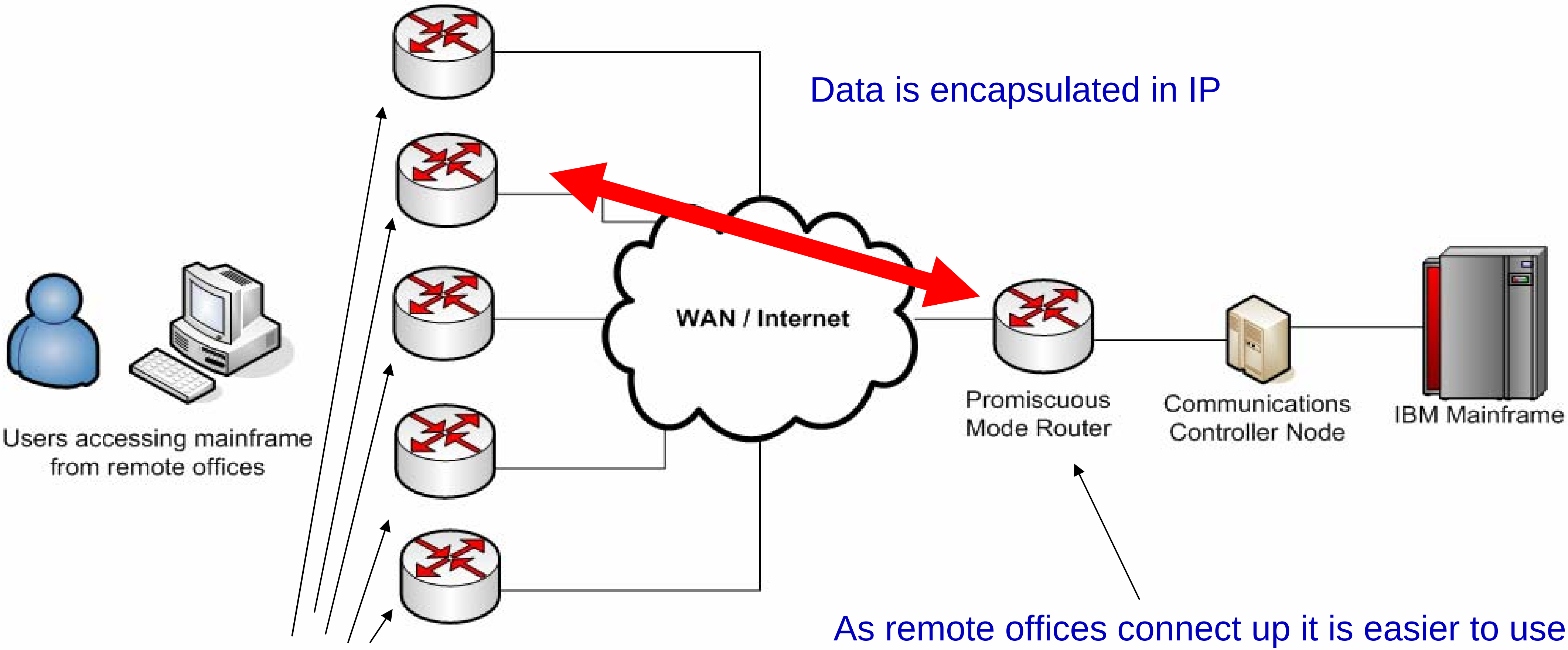
Example 3 – LLC and Bridging

SNA traffic is bridged over LLC and there is no link layer termination which is an issue if the network involves WAN links



Source Route Bridging involves routing traffic from one ring to another. If RIF is used for routing there is a 7 hop limit

Example 4 - DLSw


WAN / Internet
Users accessing mainframe from remote offices
Promiscuous Mode Router
Communications Controller Node
IBM Mainframe

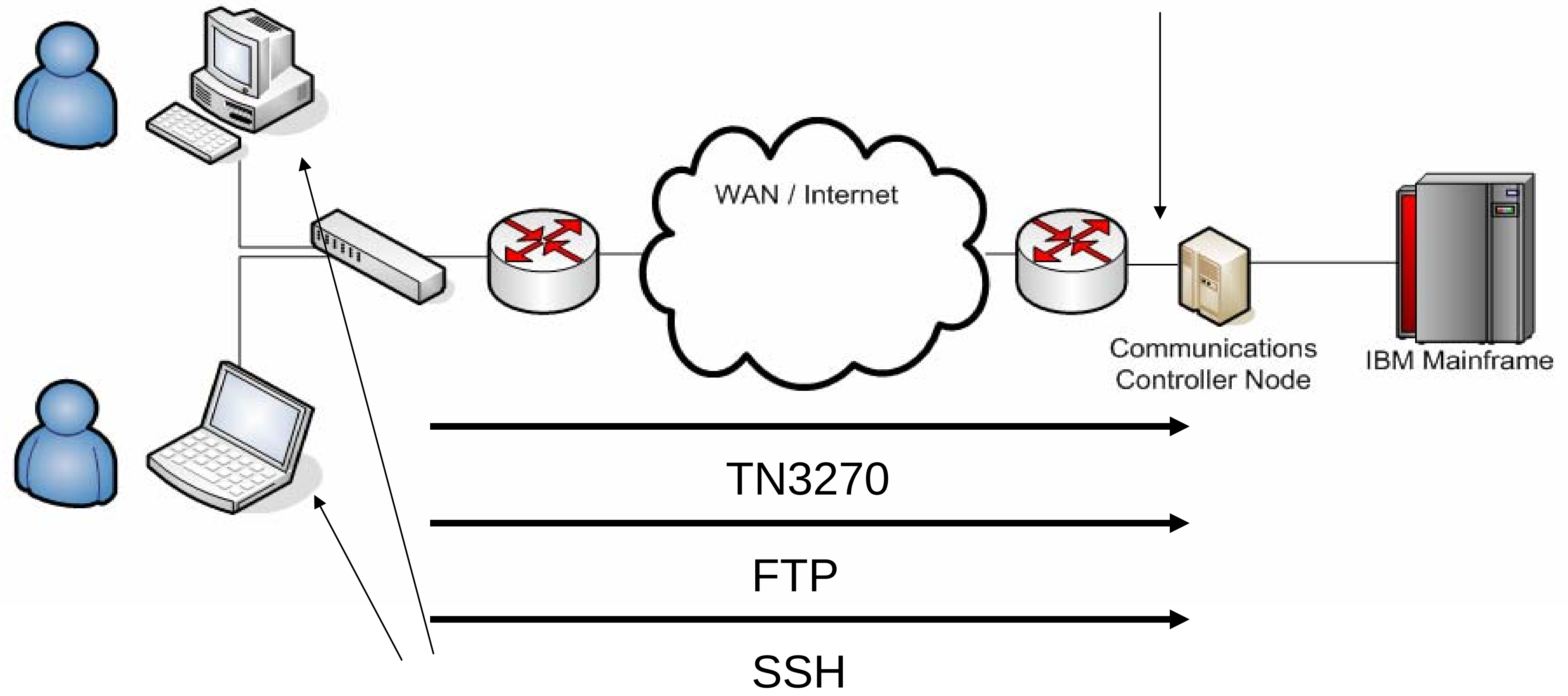
Data is encapsulated in IP

As remote offices connect up it is easier to use promiscuous mode so you are not altering the router configuration on a regular basis

Each remote office establishes a DLSw tunnel with the data centre

Example 5 – IP Services

Often a channel attachment is used to connect to the router



TN3270

FTP

SSH

Users running terminal emulation applications

Introduction to DLSw

Data Link Switching (DLSw) was initially designed by IBM and was released in 1993 in RFC 1434.

The protocol is used for “packet switching”, it encapsulates SNA or NetBIOS frames in IP and also provides local termination of the link layer.

A number of improvements were made to the protocol and were included in RFC 1795 which was released in 1995.

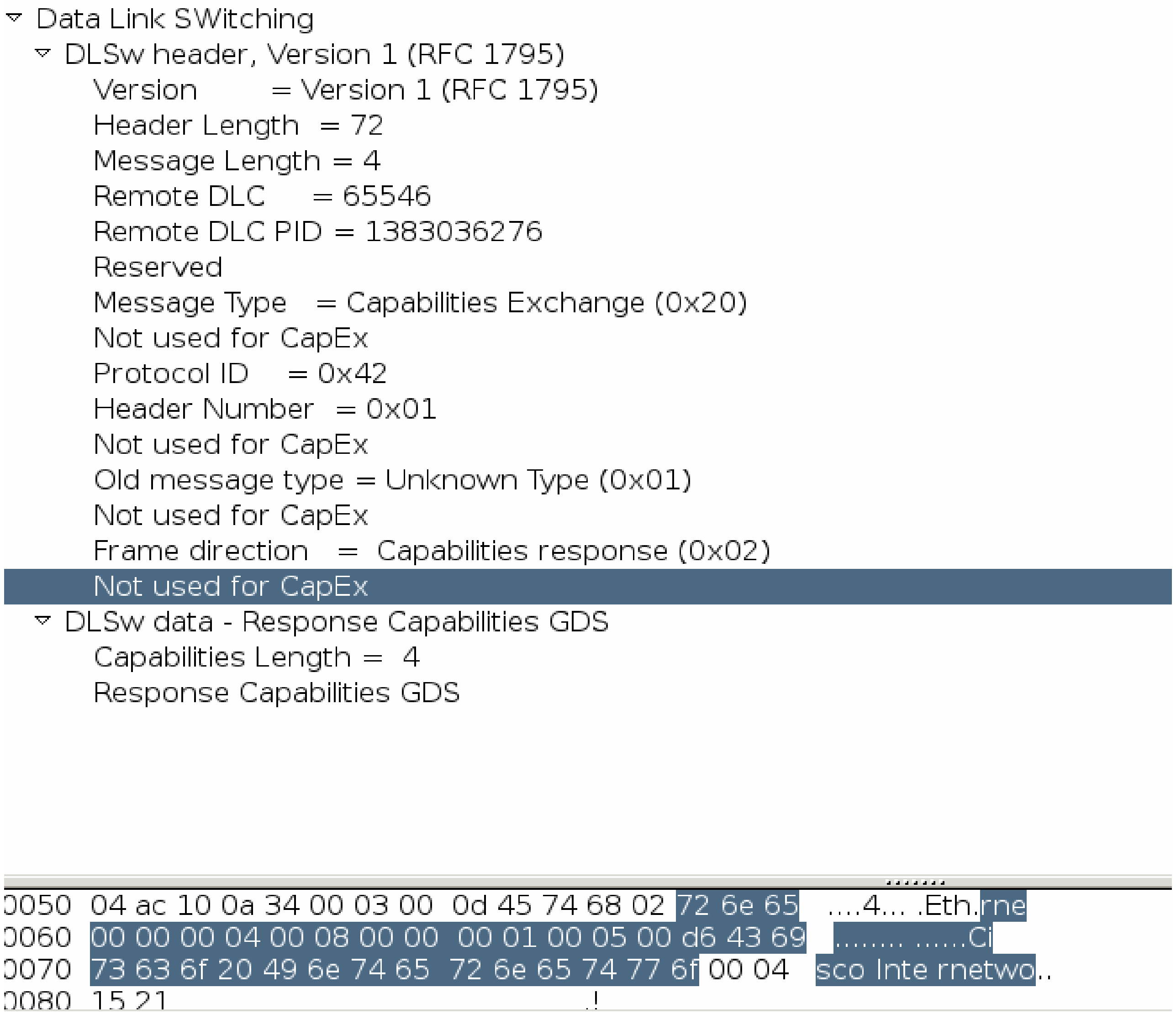
Cisco produced their own extensions to the protocol known as DLSw+ and this formed the basis of version 2 of the protocol.

Version 2 of the protocol was documented in RFC 2166 and was released in 1997. In practical terms this is the most widely adopted version.

This is not modern technology but it is still used by a large number of organisations.

Format of DLSw Headers

A Capability Exchange packet has the simplest type of DLSw Header



```
▽ Data Link SWitching
  ▽ DLSw header, Version 1 (RFC 1795)
      Version          = Version 1 (RFC 1795)
      Header Length  = 72
      Message Length = 4
      Remote DLC      = 65546
      Remote DLC PID = 1383036276
      Reserved
      Message Type    = Capabilities Exchange (0x20)
      Not used for CapEx
      Protocol ID     = 0x42
      Header Number   = 0x01
      Not used for CapEx
      Old message type = Unknown Type (0x01)
      Not used for CapEx
      Frame direction    =  Capabilities response (0x02)
      Not used for CapEx
  ▽ DLSw data - Response Capabilities GDS
      Capabilities Length =  4
      Response Capabilities GDS

0050  04 ac 10 0a 34 00 03 00  0d 45 74 68 02 72 6e 65   ....4... .Eth.rne
0060  00 00 00 04 00 08 00 00  00 01 00 05 00 d6 43 69   ........ ......Ci
0070  73 63 6f 20 49 6e 74 65  72 6e 65 74 77 6f 00 04   sco Inte rnetwo..
0080  15 21                                              .!
```

Types of DLSw Packet

- Capabilities Exchange
- CANUREACH
- ICANREACH
- XID
- Data
- Halt Data Link

Format of DLSw Capability Data

General Data Stream (GDS) is used for the format of the message portion of the packet. it is also used in APPN as well as the 5250 protocol.

Structured field: -

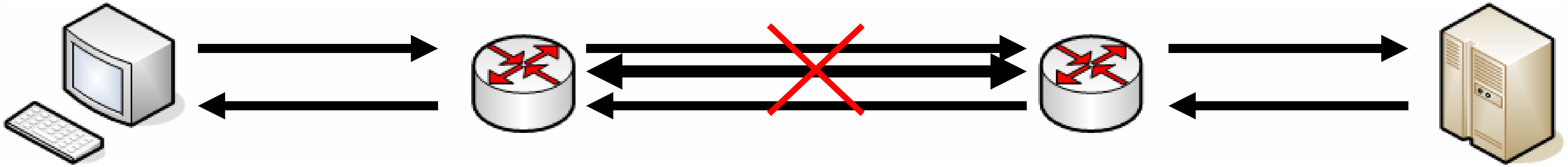
Length (LL)		Format Identifier (GDS ID)	
0x00	0x10	0x15	0x20

Standard vector block:-

Vector Length	Vector ID	Data	
0x04	0x81	0x02	0x00

DLSw Circuit Establishment

DLSw circuits are established over the TCP connections that are setup during the Capability Exchange. Multiple circuits can exist over the TCP connection and it doesn't drop even if there aren't any active circuits.



[illegible] rk bridge.
[illegible] used.
types of DLSw packet for the XID exchange and other stages of
the conversation.

Attacking

Attacker Objectives

Why attack these environments ?

- Financial data is often held in the mainframe
- The processing power of the mainframe
- It’s cool owning Heavy Metal

What do we need to gain access ?

- Access to services that provide a login and valid credentials
- A vulnerability or poor configuration of the mainframe

Objective 1 – Leak Information

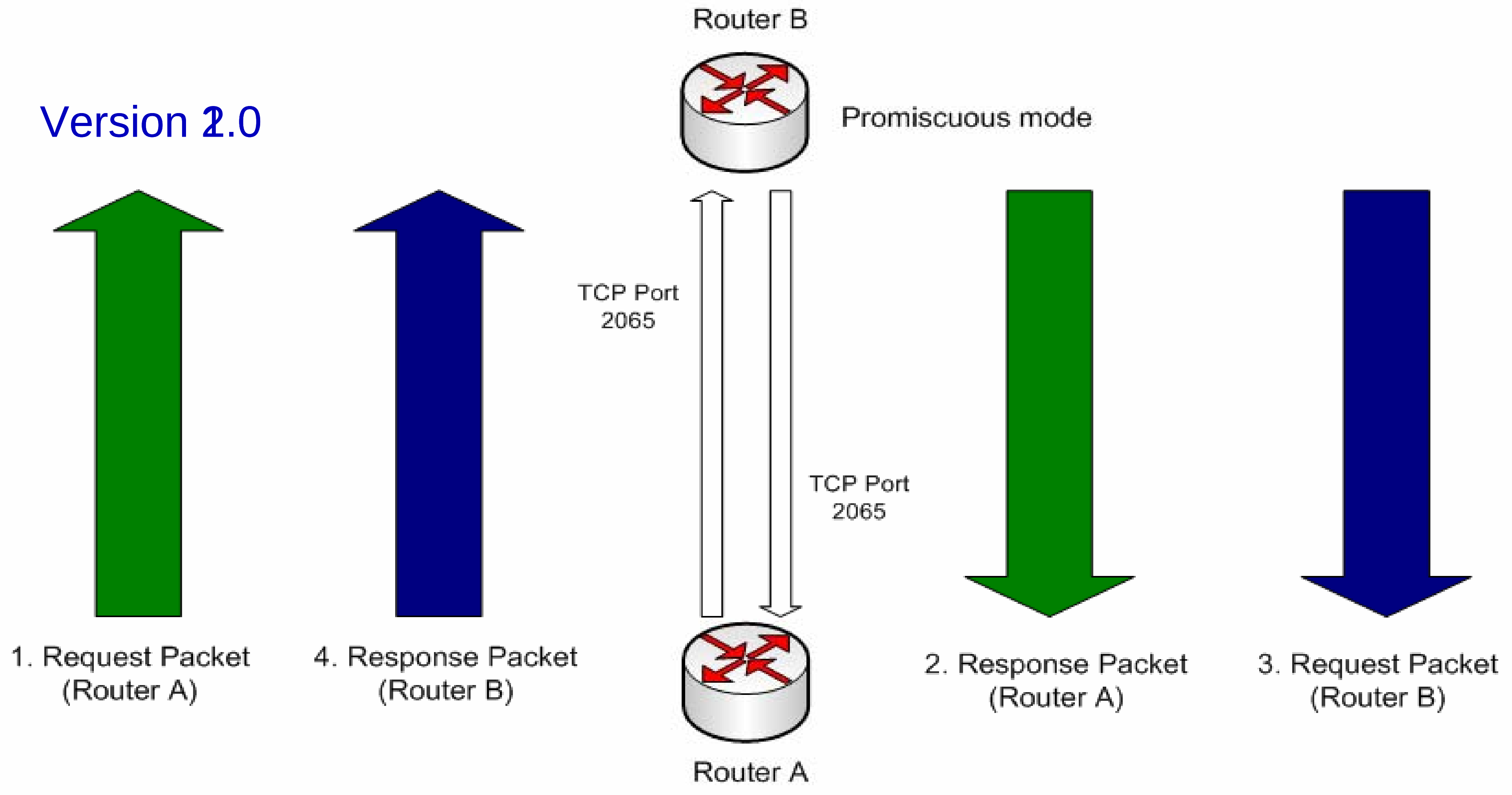
Firstly, we want to know about the DLSw configuration of the Network.

All the textbooks tell us to expect at least one router to be in “promiscuous” mode.

So what can we learn from a “promiscuous” mode router ?

Capability Exchange

Version 2.0



Once Capabilities have been exchanged DLSw circuits can be started

Information in Capability Exchange

- A router will return the following information if our IP address is defined in its configuration or it is in “promiscuous” mode.

- Mac Addresses
- NetBIOS names
- Router version information
- SAP Filtering Status
- Multicast Support
- Border Peer Support
- Pacing Information

Tools for the Job

I have released a Python script to accompany this talk, you need to use the BitVector package to run it.

It is written as an extension to Scapy to take advantage of the cool features it has.

I have written some DLSw classes for Scapy that I will be sharing once they are finished.

Alternatively you can use a DLSw capable router but you can’t control all the parameters.

DLSw Query Tool

Here is some sample output

```
####################################################################
TARGET: 192.168.0.1
PORT: 2065
DATE: Sun Apr  2 17:45:21 2006
####################################################################

DLSw Version: 2.00
TCP Connections: 1
Vendor OUI: 0x00000c Cisco
Multicast: Yes
Initial Pacing: 20

Mac Address Info:
Exclusivity: No
Address: 0090.dab8.e400 Mask: ffff.ffff.ffff
Address: 0040.adbd.8989 Mask: 0000.ffff.ffff
Address: 0000.1111.2222 Mask: 0000.ffff.ffff

NetBIOS Name Info:
Exclusivity: No
Name: SYSTEM1
Name: system2

SAP Support:
Total SAPs allowed: 128 / 128
```

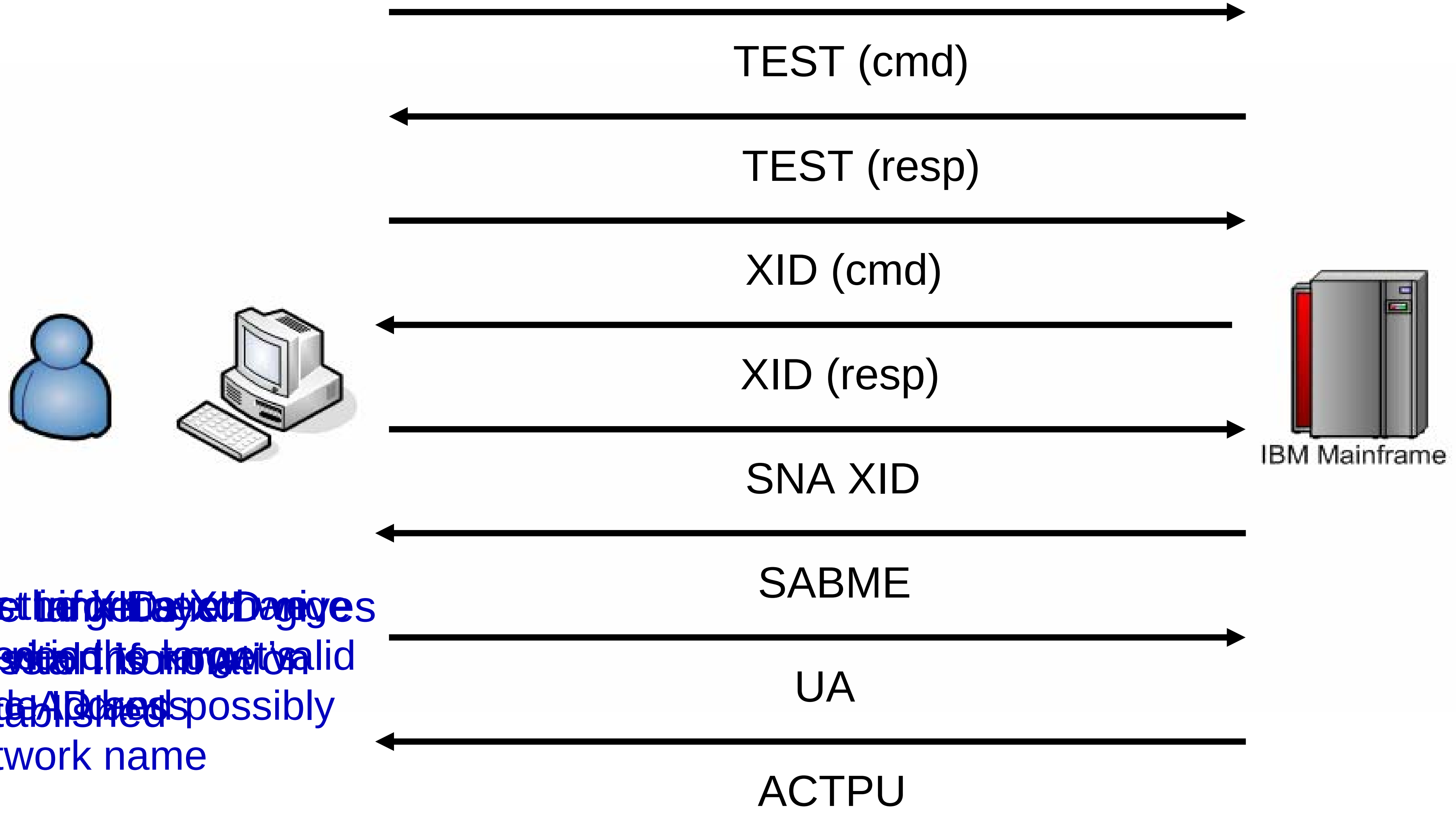
Objective 2 – Reach the Mainframe

It might not be running an IP stack so how can we access it from the Internet ?

Does an attacker on the Internet gaining access to the Mainframe logon screen breach our security model ?

We now have a DLSw tunnel to use because of a “promiscuous” mode router.

SNA Session Setup (LLC)



[illegible] XID [illegible] es

[illegible] valid

[illegible] possibly

network name

Information Discovery

- Capabilities Exchange
  - Supported SAP Types

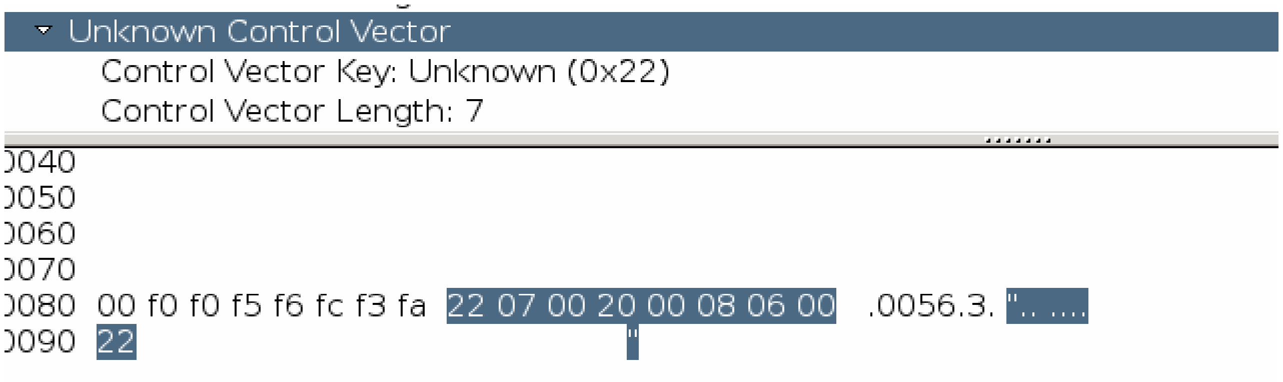
```
SAP Support:
Total SAPs allowed: 128 / 128
```

  - Mac Addresses

```
Mac Address Info:
Exclusivity: No
Address: 4000.adbd.8989 Mask: ffff.ffff.ffff
```

Information Discovery part 2

- XID Exchange
  - Failed Negotiation Indicator
    A control vector tells us if an error occurs, refer to the SNA Format manual for more information.



```
▾ Unknown Control Vector
      Control Vector Key: Unknown (0x22)
      Control Vector Length: 7
)040
)050
)060
)070
)080  00 f0 f0 f5 f6 fc f3 fa  22 07 00 20 00 08 06 00   .0056.3. ".. ....
)090  22                                                 "
```

  - Returned Information
    If the exchange was unsuccessful the host can potentially return the CP Name, Network ID and Node ID in the response.

Summary of the Requirements

MAC Address of Mainframe

- Capabilities Exchange
- Brute force
- Social Engineering
- Traffic sniffing
- Compromise router

CPNAME and Network ID

- Social Engineering
- Brute Force
- Traffic Sniffing
- Mainframe gives you it

Is this information usually protected in your company ?

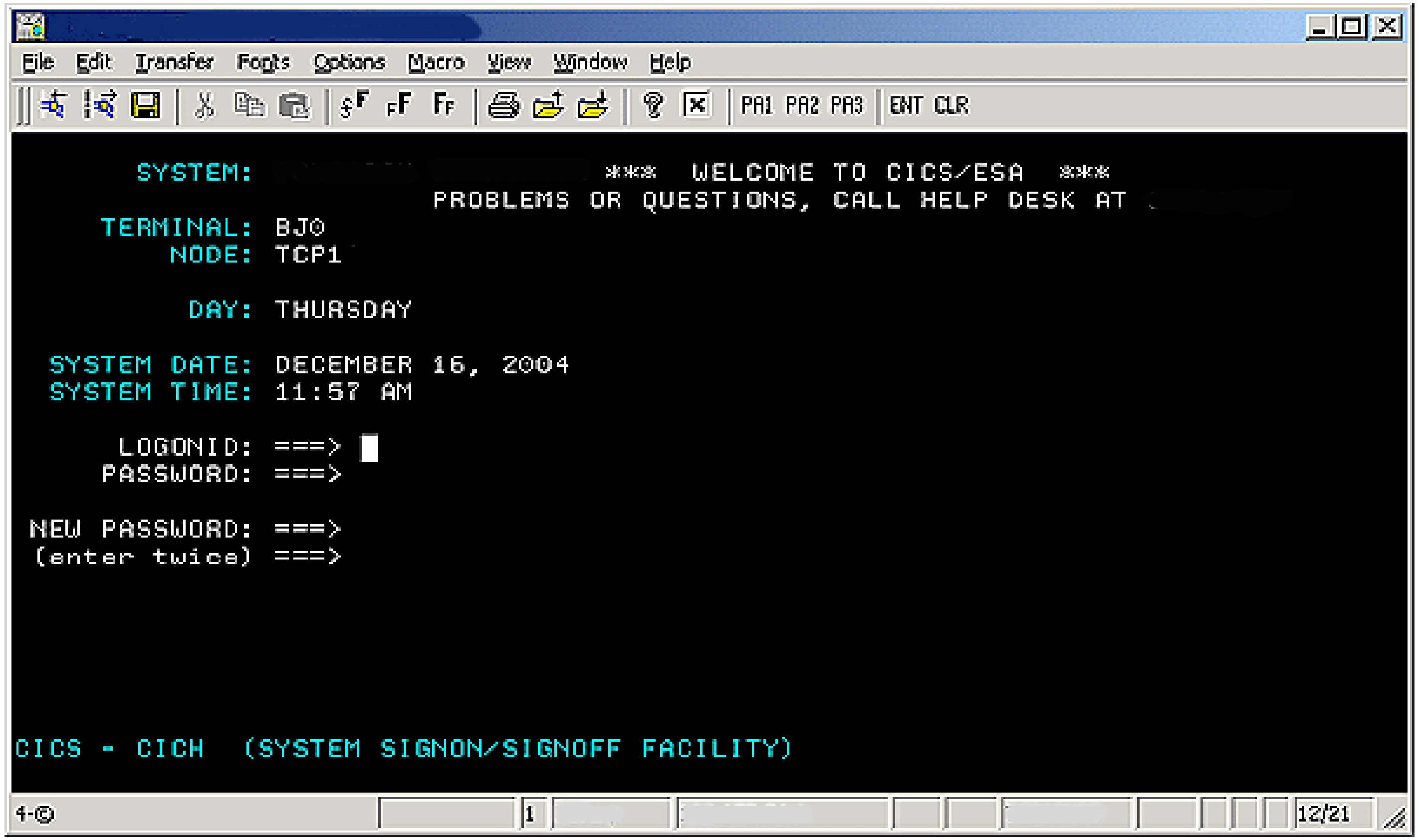
Tools for the Job

- Commercial Software
  - PCOMM
  - RUMBA

- Homemade Scripts - Scapy
  - Perfect for brute force testing and fuzzing
  - SNA and DLSw packet definitions can help
  - We will talk more about this as we go along

Access the Mainframe

We now have all the information and facilities required to access the logon screen on the mainframe



```
         SYSTEM: [redacted]          ***  WELCOME TO CICS/ESA  ***
                              PROBLEMS OR QUESTIONS, CALL HELP DESK AT [redacted]
       TERMINAL: BJ0
           NODE: TCP1

            DAY: THURSDAY

    SYSTEM DATE: DECEMBER 16, 2004
    SYSTEM TIME: 11:57 AM

        LOGONID: ===> █
       PASSWORD: ===>

   NEW PASSWORD: ===>
  (enter twice) ===>




CICS - CICH  (SYSTEM SIGNON/SIGNOFF FACILITY)
```

We just need login credentials, how can we get them ?

Remember Memory Padding Issues ?

Vulnerabilities that arise where uninitialised memory is read

- Ethernet frame padding information leakage
- Etherleak on Windows Network Card Drivers
- Microsoft Windows NetBIOS Information Leakage
- ICMP data padding on Linux
- MySQL Anonymous Handshake Information Disclosure

A useful application - SNAleak

- Usually the packets on the local network are bridged and DLSw switched so Etherleak is a factor even remotely.
- If the Routers aren’t patched they can leak information from other DLSw circuits.
- You might just find someone’s password in your packet.

SNAleak Details

- The issue is that SNA packets can be less than the minimum Ethernet frame size of 46 bytes.
- For example the LLC header, Transmission Header and Request Response Headers only total 27 Bytes.
- “Start Data Transfer” is only a single byte instruction “\xA0” so the frame will be padded.
- Generate lots of small packets from the target and you will get lots of leaked data.

Exploiting SNAleak

- Scapy is the perfect tool for exploiting this condition.
- If you write some SNA classes (or ask me nicely) you can put together attack scripts to achieve this.
- Remember to convert the leaked data from EBCDIC

Objective 3 – Exploit the router

- If we can get on the router we will be able to sniff traffic and avoid any advanced attacks.

- Don’t complicate things unnecessarily when attacking any environment, always take the easiest route.

Basic Router Security

- Look at the ports that are open on the router, if there is an easy way to compromise it try that first.
  - There are lots of vulnerabilities that could get you access to a Cisco router.
    (eg SNMP, Telnet, HTTP, TFTP, IPv6)
  - Just because mainframe environment is high availability doesn’t mean you shouldn’t patch routers.
  - If using failover routers it is easy to upgrade IOS and test redundancy.
- If you see TCP ports 2065 and 2067 the router is probably running DLSw.

DLSw related vulnerabilities

- In a high availability environment even a small outage can potentially cost lots of money.

- Described here is one DoS that needs further investigation.

Cisco Vulnerability

DETAILS OF NEW CISCO VULNERABILITY TO BE ADDED HERE

Objective 4 – Redirecting Traffic

Scenario 1 - Local Attack

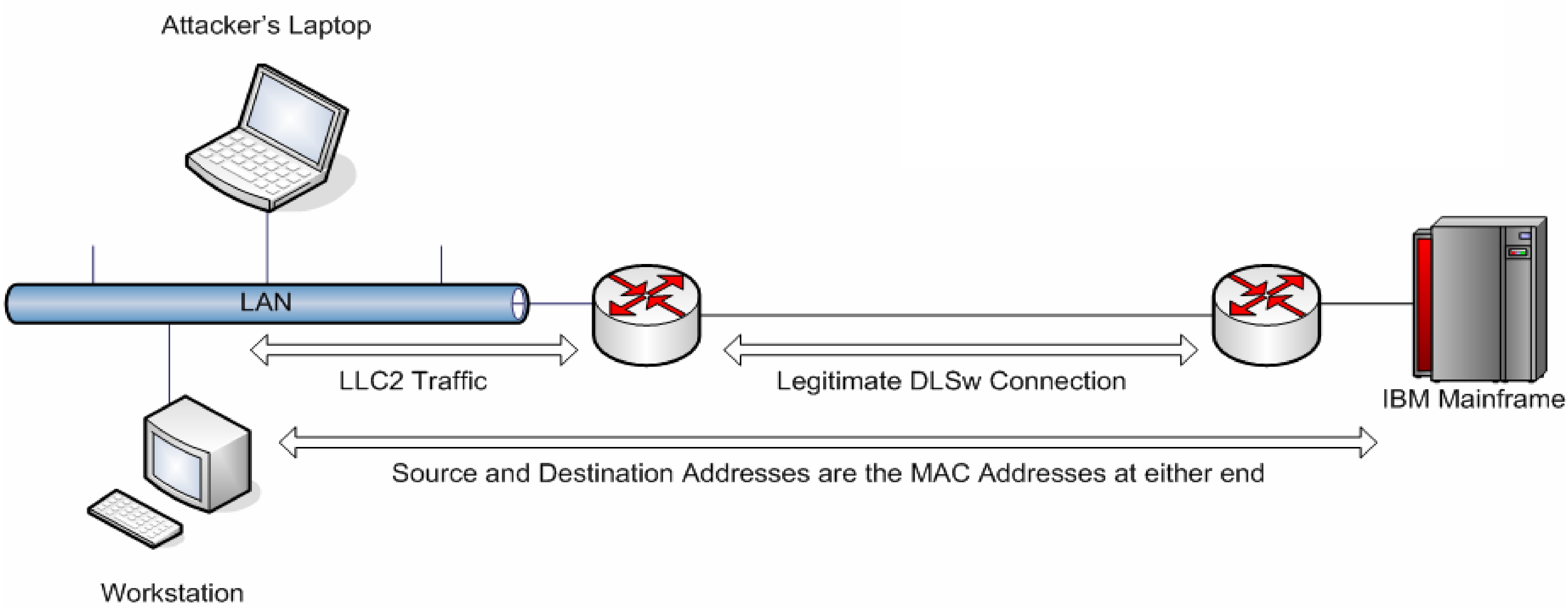
This attack is dependent on the architecture but this example uses a setup that is very common on internal networks.

The attack assumes the SNA traffic is using LLC2 at the link layer.

The attack enables us to intercept the network traffic from other systems plugged into the same switch as we are.

MWR InfoSecurity

Local Attack – Before


Attacker's Laptop
LAN
LLC2 Traffic
Legitimate DLSw Connection
IBM Mainframe
Source and Destination Addresses are the MAC Addresses at either end
Workstation

Local Attack - Issues

An attacker needs to be able to intercept the LLC2 traffic on the local LAN.

A CAM Table Overflow against the switch or an attack against the workstation are valid.

If these aren’t possible we don’t have the luxury of ARP spoofing as we aren’t using IP.

What about using port stealing to get the traffic?

Port Stealing

Marco Valleri and Alberto Ornaghi demonstrated the technique in 2003. The attack involves stealing the target's MAC address, then sending the intercepted data on to the real system.

It can be used to bypass static ARP and could potentially work in the scenario we have constructed.

It requires a target to be running IP as we need to use a spoofed ARP packet to give the target its port back. Therefore only a half duplex attack is possible if the target workstation has a working IP stack.

We still can't get login credentials as the target mainframe probably won't have an IP address associated with the target MAC address and we can only get half duplex.

Local Attack - Requirements

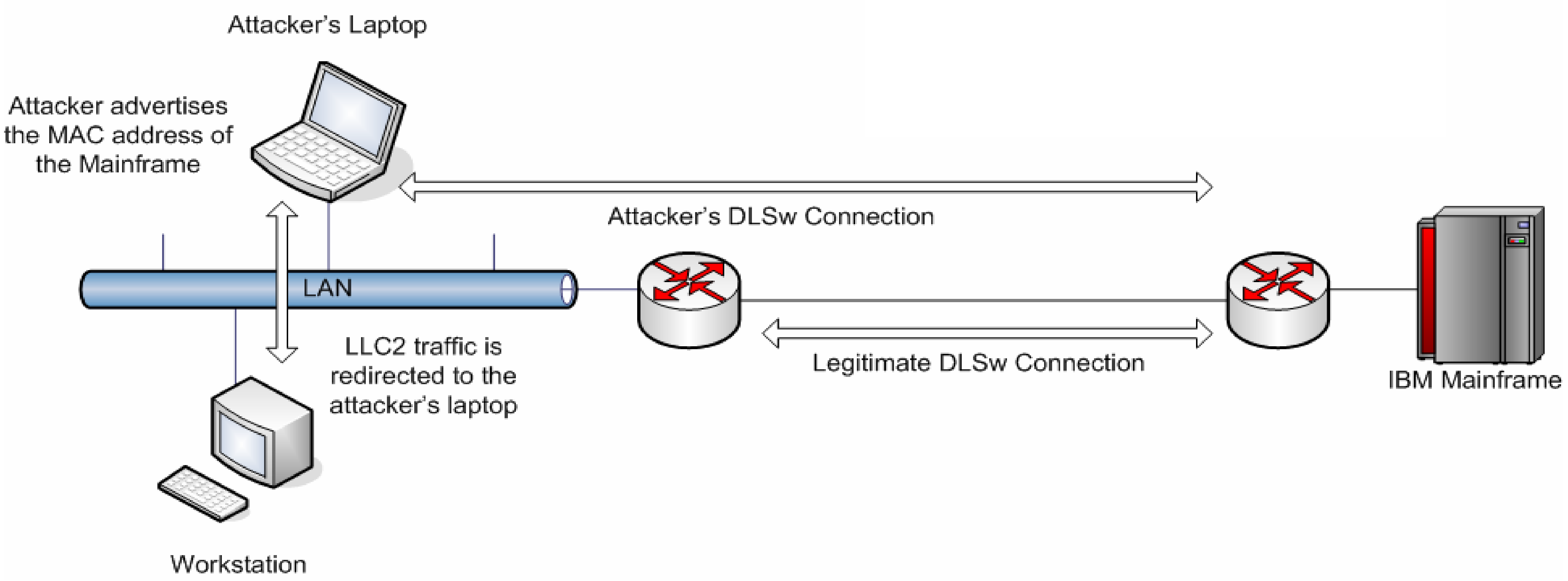
If we can use DLSw to provide the transport we can sniff the traffic on a single switch.

It is best to use two network cards, one with the mainframe’s MAC address and the other for the DLSw connection.

All LLC2 data we receive is encapsulated and passed as IP down a DLSw connection to the promiscuous mode router.

We can now sniff the application data including credentials for the mainframe.

Local Attack – After


Attacker's Laptop
Attacker advertises the MAC address of the Mainframe
Attacker's DLSw Connection
LAN
LLC2 traffic is redirected to the attacker's laptop
Legitimate DLSw Connection
IBM Mainframe
Workstation

Redirecting Traffic – Part 2

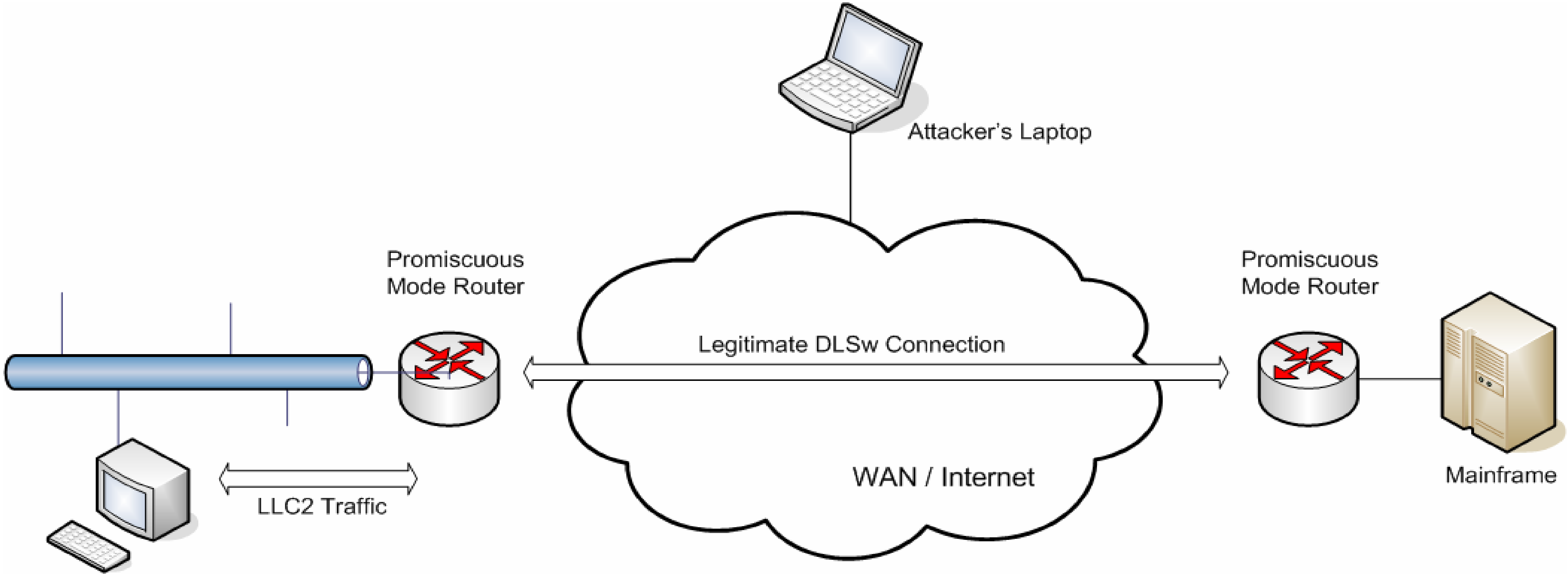
Scenario 2 – Remote Attack

This attack is dependent on the architecture but is possible if the DLSw configuration of the routers at both ends of the "tunnel" is not secure.

This assumes our SNA traffic is using DLSw to traverse an IP network.

We need to find two routers that are configured in promiscuous mode, one in front of the mainframe and one at the user's end.

Remote Attack - Before



Remote Attack - Issues

If we can sniff the IP traffic using a traditional method this attack isn’t needed.

We need to be able to open DLSw connections to the routers at both ends of the conversation.

Either our IP address must be defined in each router’s configuration or they must both be in promiscuous mode.

If a circuit has already been established between two hosts this won’t work (by default the circuit will drop after roughly 15 minutes of inactivity).

Remote Attack - Requirements

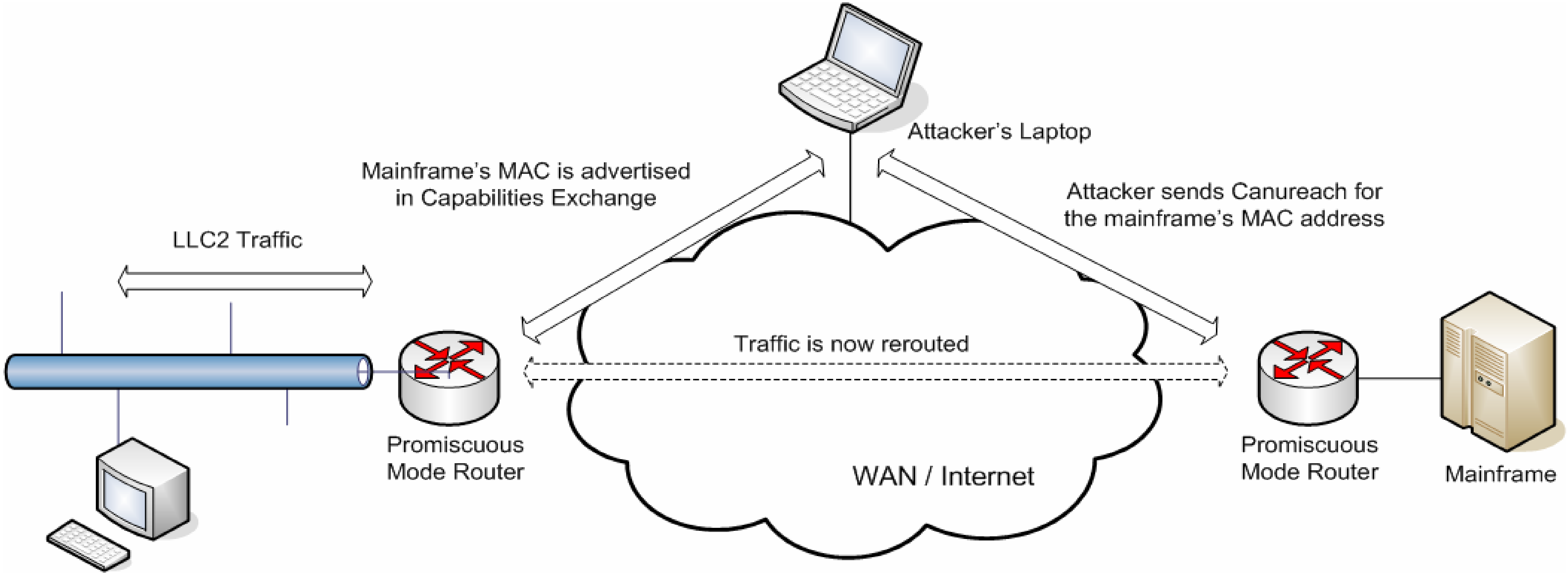
We need to exchange capabilities with the routers at either end of the legitimate DLSw connection.

We need to advertise the MAC addresses of the hosts we want to intercept traffic for.

A lower path cost could be advertised or if there are peer groups defined we could become a new border peer.

Gratuitous ICANREACH is possible but this won’t override Capability Exchange information.

Remote Attack - After



Recommendations

Technical Recommendations

- Don’t use promiscuous mode on any router.
- Where possible have MAC addresses explicitly defined in the capabilities exchange.
- Use the lowest possible path costs when defining links.
- Specifically protect port 2065 with filtering using firewalls and router ACLs.
- Use IPSec to protect DLSw traffic between routers.

Technical Recommendations – part 2

- Ensure end-to-end encryption for the data that is traversing the network.

- Use the SSL and SSH support on the mainframe if IP is the right solution.

- Keep each component of the network patched to the latest level.

- Make sure the SNA gateway is “hardened” if that communication model is being used.

High Level – Part 1

- Understand the protocols in use and their strengths and weaknesses
  - § Is host authentication supported ?
  - § Can encryption be used ?
  - § Are traffic redirection attacks possible ?
  - § Understand all aspects of your network not just IP.

- Deploy an architecture that provides the required security features
  - § Maintain control over the accessibility of all services
  - § Ensure patching can occur with minimal disruption
  - § Monitor for suspicious activity
  - § Ensure that data remains private

High Level – Part 2

Ensure security testing is thorough

- Make sure pen testers don’t just know about IP
- A combination of manual testing and security consultancy should be used where possible

Get everyone talking to each other

- Desktop team / Network Team / Mainframe operators
- Educate everyone about security issues
- Use the security team to co-ordinate initiatives
- Be proactive in improving security

So are we safe now ?

Maybe not! There is still lots more work to be done

- Fuzzing more protocol stacks
- DLSw stack for Linux
- Investigating SNA TOS handling
- Host Integration Server / NetWare for SAA
- APPN / APPC attacks
- Secure VTAM configuration

Summary

- The topology and construction of your network determine what the risks are.
- There are weaknesses in the technologies commonly deployed to enable access to mainframes.
- The risks must be understood and then mitigated.

Request for Help

- It is difficult to research this subject without access to a mainframe or other SNA host.
- Lots of work is still to be done and I would love to work with other people on this.
- Let me know if you are interested !

References and Further Reading

- IBM Networking

  http://publib.boulder.ibm.com/infocenter/zoslnctr/v1r7/index.jsp?topic=/com.ibm.znetwork.doc/znetwork_5.html

- Port Stealing

  http://www.blackhat.com/presentations/bh-europe-03/bh-europe-03-valleri.pdf

- Etherleak

  http://www.kb.cert.org/vuls/id/471084
  http://www.securitytracker.com/alerts/2003/Jun/1006959.html
  http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0001
  http://www.securityfocus.com/bid/8532/discuss

References and Further Reading – part 2

- DLSw

  http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/dlsw.htm

- RFCs

  1434

  1795

  2166

- Books

  Demystifying SNA – Taylor

  SNA Interconnections – Chiong

  IBM SNA Protocol Manual

Questions ?