Chapter 11

Network Management Applications

All sections included except the 3 first correlation techniques

Objectives

- Network management and system management
- Network management
  - Configuration
  - Fault
  - Performance
  - Security
  - Accounting
- Configuration management
  - Configuration management
  - Service/Network provisioning
  - Inventory management
- Fault management
  - Fault detection and isolation
  - Correlation techniques for root cause analysis
- Performance management
  - Performance metrics
  - Data monitoring
  - Problem isolation
  - Performance statistics

(continued)

Objectives (cont.)

- Security management
  - Security policies and procedures
  - Security threats
  - Firewall
  - Cryptography: keys, algorithms, authentication, and authorization schemes
  - Secure message transfer methods
- Accounting management
- Report management
- Policy-based management
- Service level management
  - Quality of service, QoS
  - Service level agreement, SLA

Network and Systems Mgmt

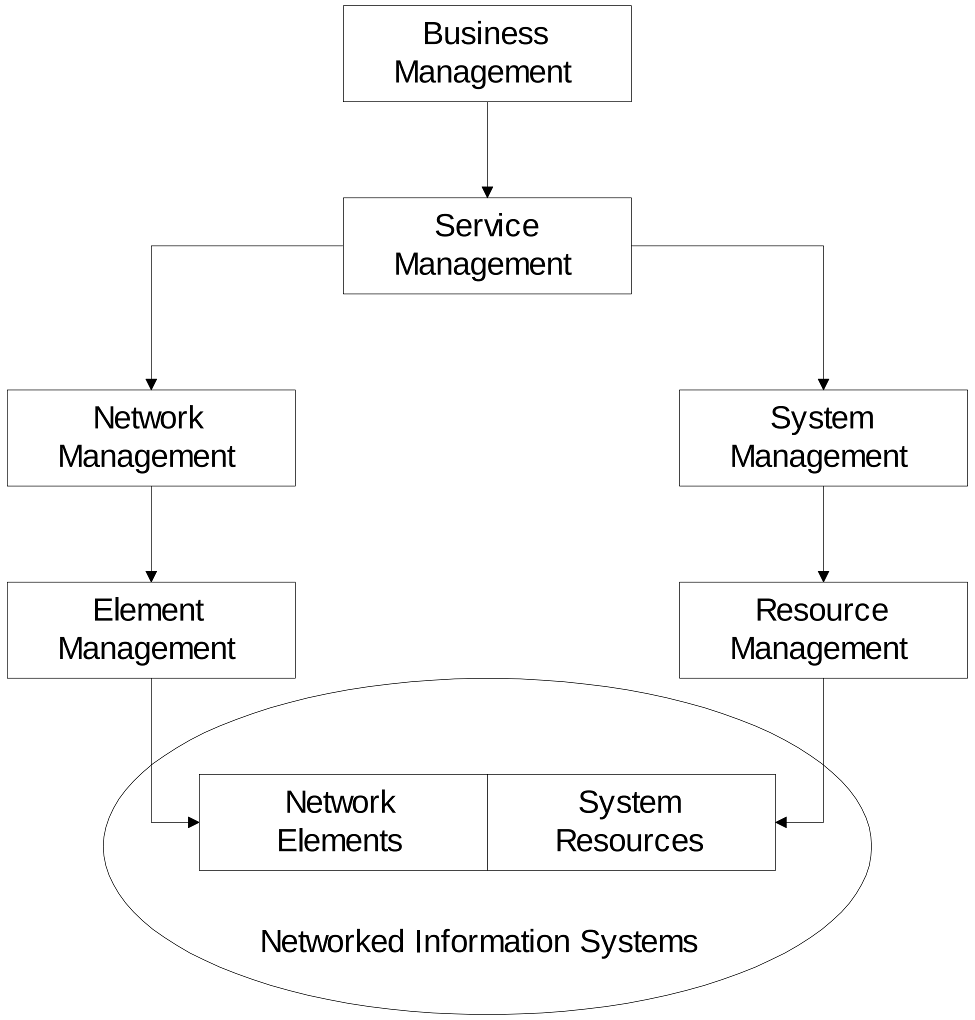


Figure 11.1 Network and System Management

Notes

- TMN architecture expanded to include systems management

Management Applications

- OSI Model
    - Configuration
    - Performance
    - Fault
    - Security
    - Accounting
- Reports
- Service Level Management
- Policy-based management

Notes

Configuration Management

- Network Provisioning (making it available)
- Inventory Management
  - Equipment
  - Facilities
- Network Topology
- Database Considerations

Notes

Circuit Provisioning

- Network Provisioning
  - Provisioning of network resources
    - Design
    - Installation and maintenance
  - Circuit-switched network
  - Packet-switched network, configuration for
    - Protocol
    - Performance
    - QoS
  - ATM networks

Notes

- Examples:
  - TIRKS (Trunk Integrated Record Keeping System) for circuit-switched networks
  - E1 in TIRKS for equipment management
  - F1 in TIRKS for facilities management

Network Topology

- Manual
- Autodiscovery by NMS using
  - Broadcast *ping*
  - ARP table in devices
- Mapping of network
  - Layout
  - Layering
- Views
  - Physical
  - Logical

Notes

Traditional LAN Configuration

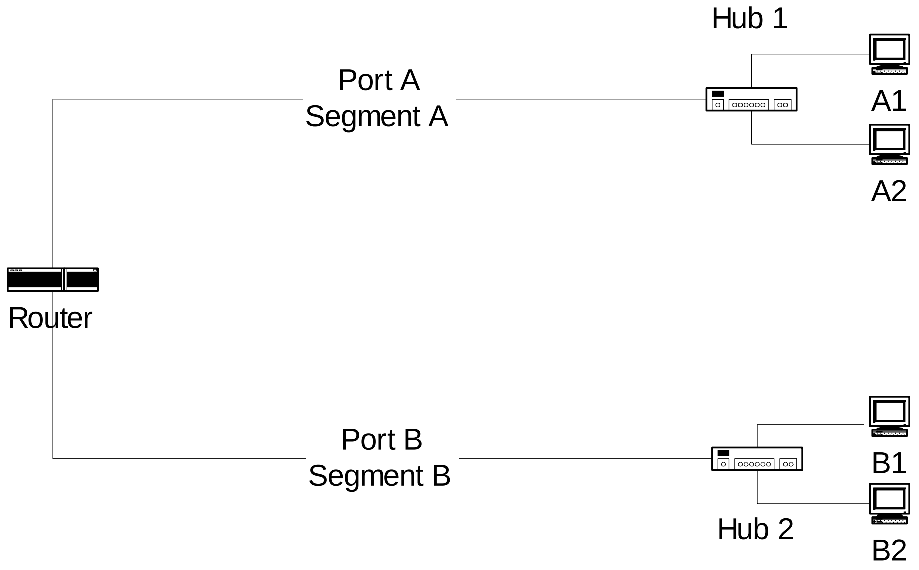


Figure 11.2 LAN Physical Configuration

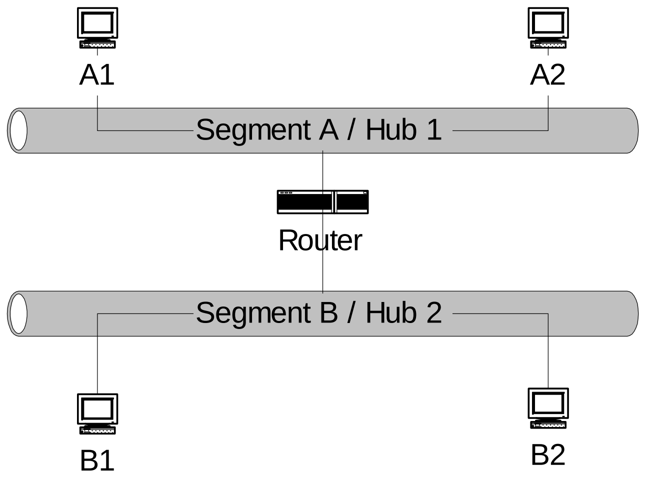


Figure 11.3 Logical Configuration of Two LAN Segments

Notes

- One-to-one mapping between physical and logical configuration

Virtual LAN Configuration

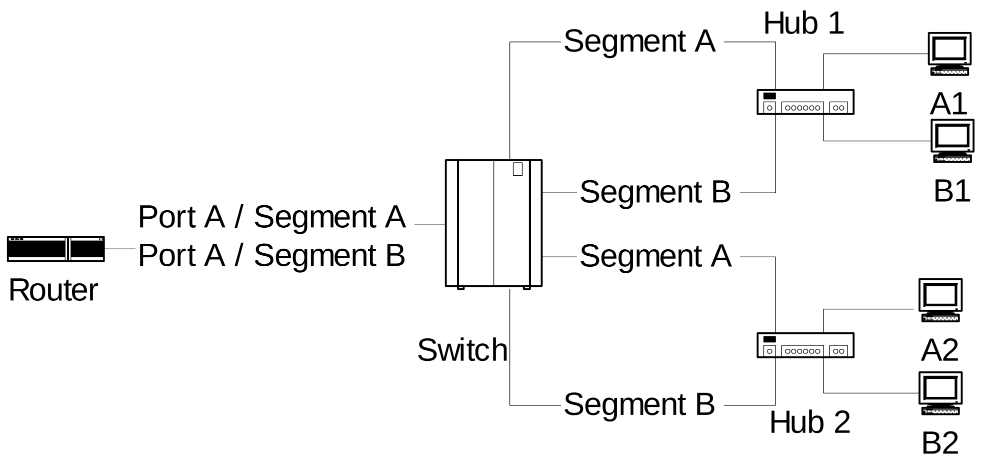


Figure 11.4 VLAN Physical Configuration

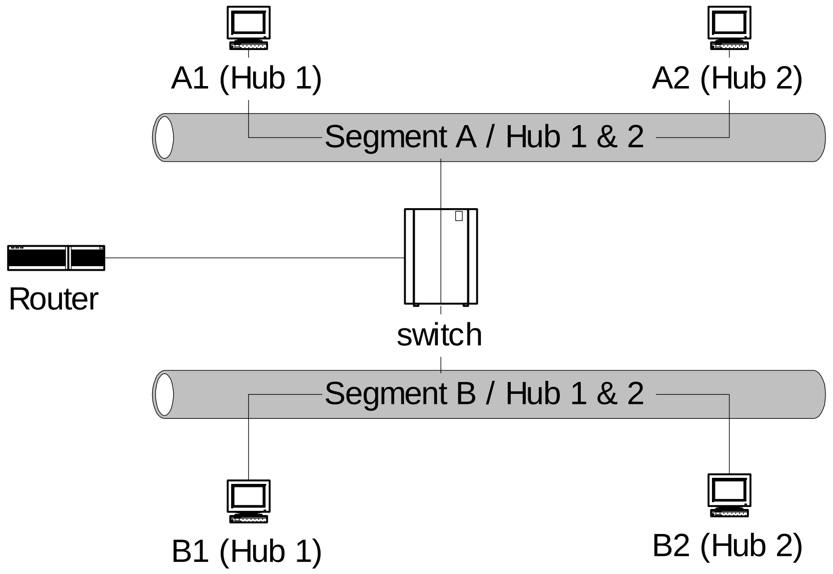


Figure 11.5 Logical Configuration of Two VLAN Segments

Notes

- Physical and logical configurations different
- Physical location obtained from System group

Fault Management

- Fault is a failure of a network component
- Results in loss of connectivity
- Fault management involves:
  - Fault detection
    - Polling
    - Traps: *linkDown, egpNeighborLoss*
  - Fault location
    - Detect all components failed and trace down the tree topology to the source
    - Fault isolation by network and SNMP tools
    - Use artificial intelligence / correlation techniques
  - Restoration of service
  - Identification of root cause of the problem
  - Problem resolution

Notes

Performance Management

- Tools
- Performance Metrics
- Data Monitoring
- Problem Isolation
- Performance Statistics

Notes

- Tools:
  - Protocol analyzers
  - RMON
  - MRTG

Performance Metrics

- Macro-level
  - Throughput
  - Response time
  - Availability
  - Reliability
- Micro-level
  - Bandwidth
  - Utilization
  - Error rate
  - Peak load
  - Average load

Notes

Traffic Flow Measurement Network Characterization

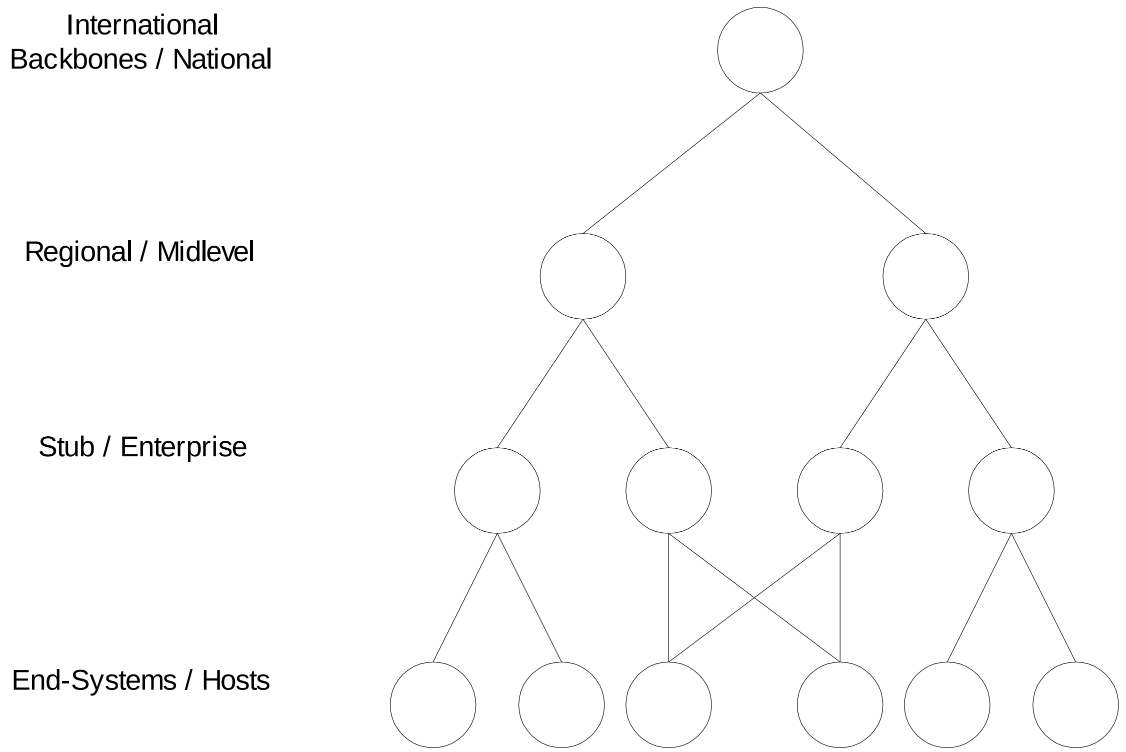


Figure 11.6 Traffic Flow Measurement Network Characterization

Notes

- Four levels defined by IETF (RFC 2063)
- Three measurement entities:
  - Meters gather data and build tables
  - Meter readers collect data from meters
  - Managers oversee the operation
- Meter MIB (RFC 2064)
- NetrMet - an implementation (RFC 2123)

Data Monitoring and Problem Isolation

- Data monitoring
  - Normal behavior ()
  - Abnormal behavior (e.g., excessive collisions, high packet loss, etc.)
  - Set up traps (e.g., parameters in alarm group in RMON on object identifier of interest)
  - Set up alarms for criticality
  - Manual and automatic clearing of alarms

- Problem isolation
  - Manual mode using network and SNMP tools
  - Problems in multiple components need tracking down the topology

  - **Automated mode using correlation technology**

Notes

Performance Statistics

- Traffic statistics
- Error statistics
- Used in
    - QoS tracking
    - Performance tuning
    - Validation of SLA
    - Trend analysis
    - Facility planning
    - Functional accounting

Notes

Event Correlation Techniques

- Basic elements
  - Detection and filtering of events
  - Correlation of observed events using ARTIfiCIAL Intelligence
  - Localize the source of the problem
  - Identify the cause of the problem

- Techniques
  - Rule-based reasoning
  - Model-based reasoning
  - Case-based reasoning
  - **Codebook correlation model**
  - **State transition graph model**
  - **Finite state machine model**

Notes

Codebook Correlation Model: Generic Architecture

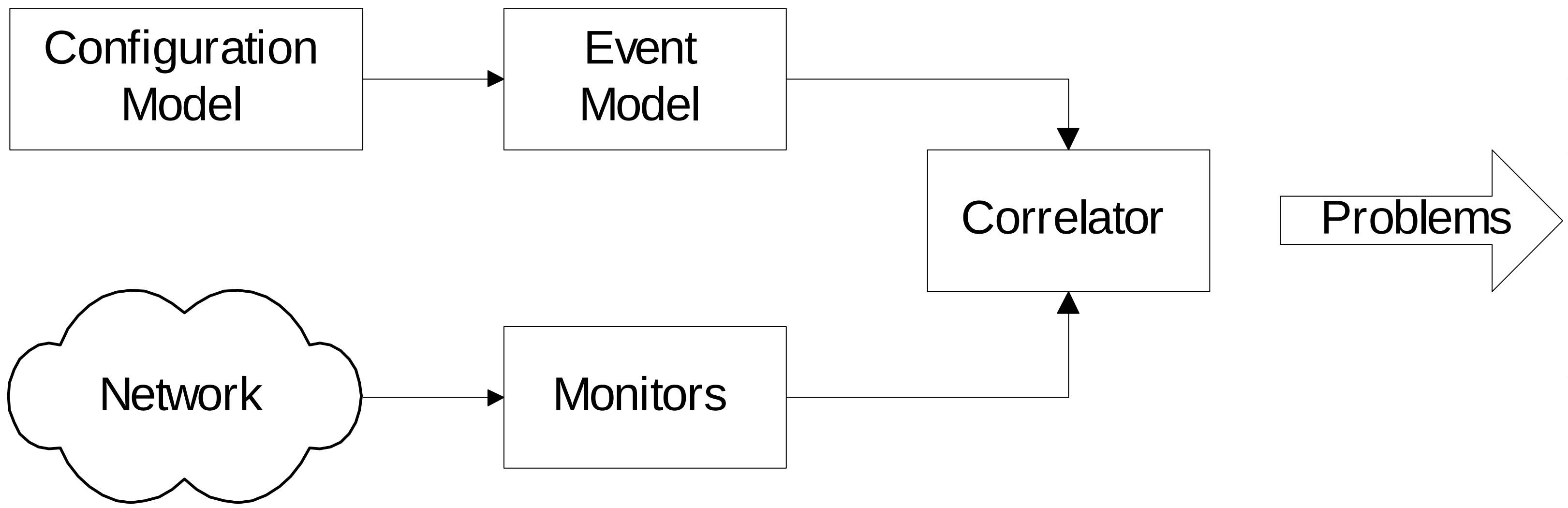


Figure 11.18 Generic Architecture of an Event Correlation System

Notes

- Yemini, et. al. proposed this model
- Monitors capture alarm events
- Configuration model contains the configuration of the network
- Event model represents events and their causal relationships
- Correlator correlates alarm events with event model and determines the problem that caused the events

Codebook Approach

Approach:

- Correlation algorithms based upon coding approach to even correlation
- Problem events viewed as messages generated by a system and *encoded* in sets of alarms
- Correlator *decodes* the problem messages to identify the problems

Two phases:

1. Codebook selection phase: Problems to be monitored identified and the symptoms they generate are associated with the problem. This generates codebook (problem-symptom matrix)

2. Correlator compares alarm events with codebook and identifies the problem.

Causality Graph

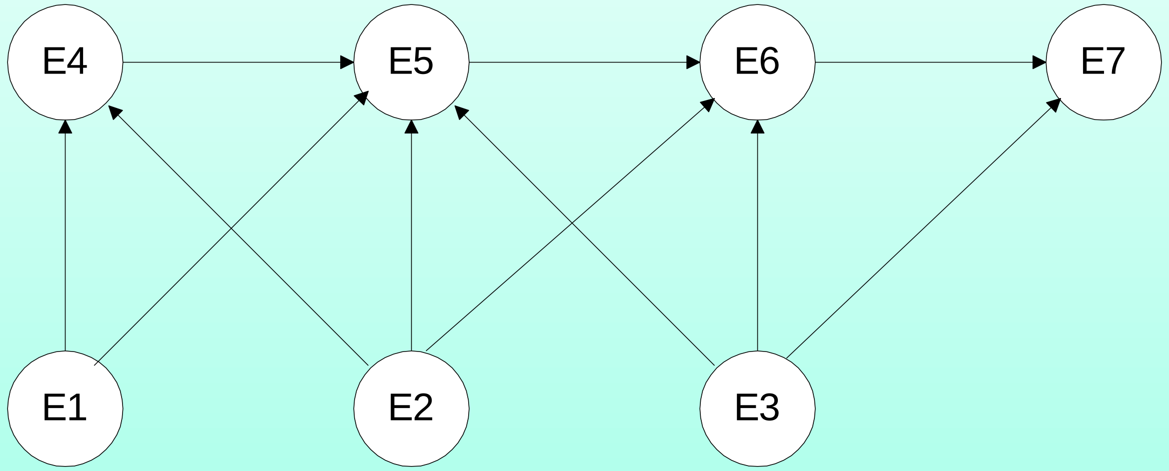


Figure 11.19 Causality Graph

Notes

- Each node is an event
- An event may cause other events
- Directed edges start at a causing event and terminate at a resulting event
- **Picture causing events as problems and resulting events as symptoms**

Labeled Causality Graph

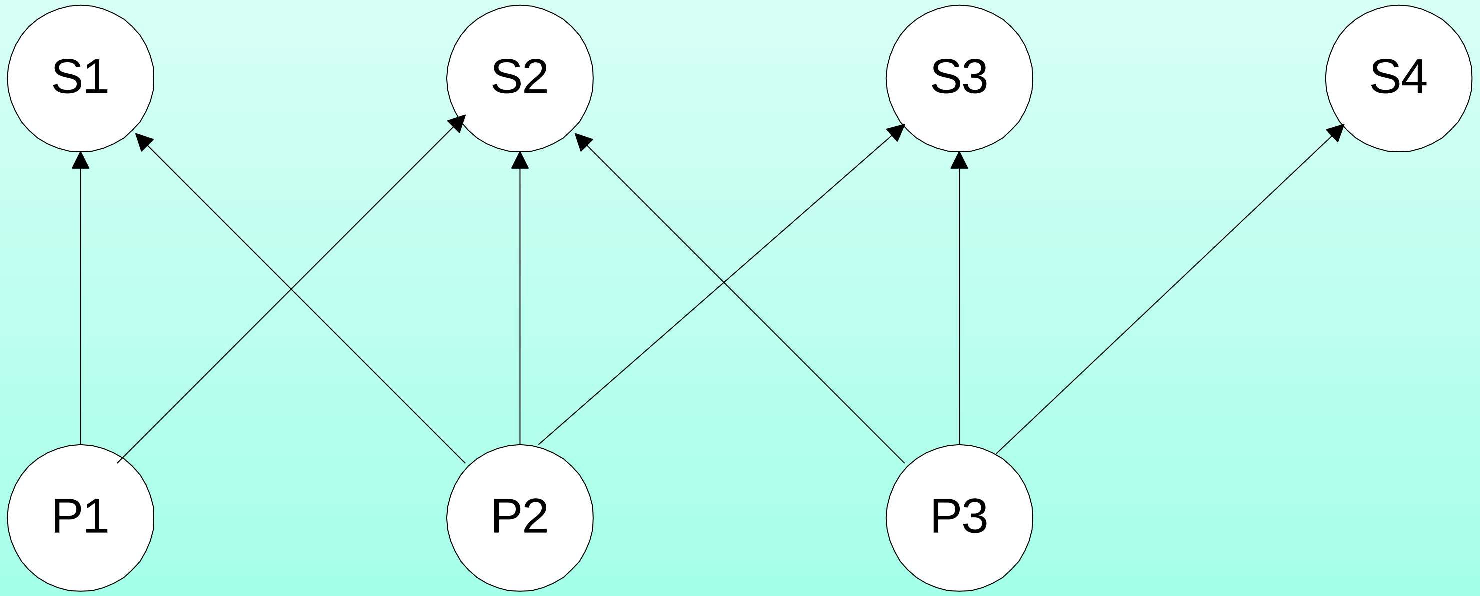


Figure 11.20 Labeled Causality Graph for Figure 11.19

Notes

- Ps are problems and Ss are symptoms
- P1 causes S1 and S2
- **Note directed edge from S1 to S2 removed; S2 is caused directly or indirectly (via S1) by P1**
- S2 could also be caused by either P2 or P3

Codebook

	P1	P2	P3
S1	1	1	0
S2	1	1	1
S3	0	1	1
S4	0	0	1

Figure 11.21 Codebook for Figure 11.20

Notes

- Codebook is problem-symptom matrix
- It is derived from causality graph after removing directed edges of propagation of symptoms
- Number of symptoms => number of problems
- 2 rows are adequate to uniquely identify 3 problems

Correlation Matrix

	P1	P2	P3
S1	1	1	0
S3	0	1	1

Figure 11.22 Correlation Matrix for Figure 11.20

Notes

- Correlation matrix is reduced codebook

Correlation Graph

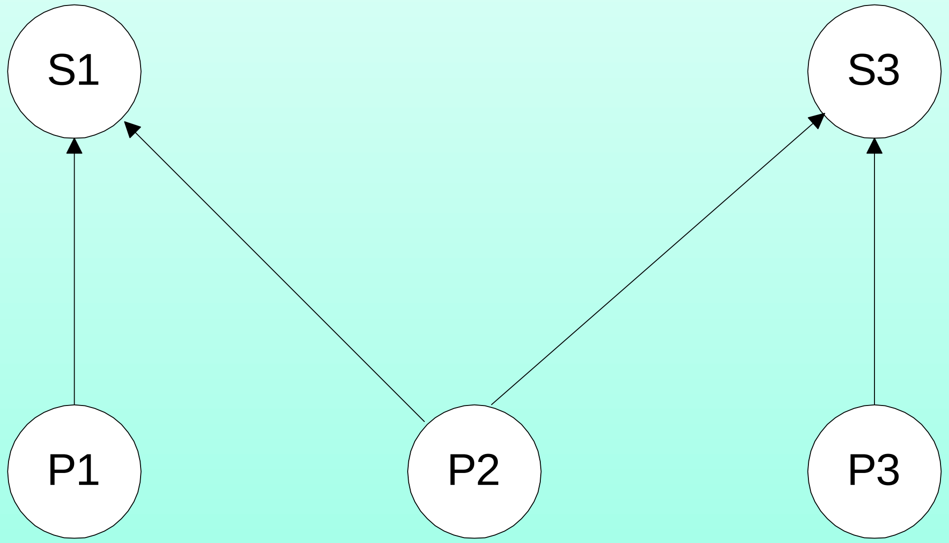


Figure 11.23 Correlation Graph for Figure 11.20

Notes

- Correlation graph is derived from correlation matrix

Generalized Causality Graph

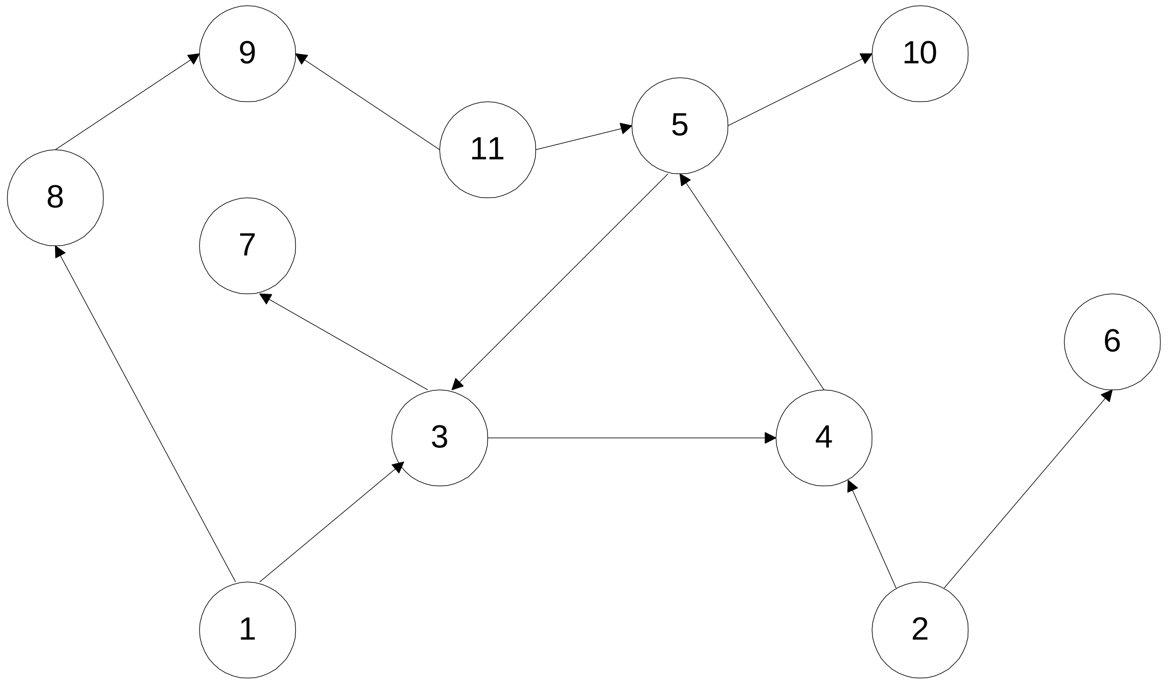


Figure 11.24(a) Event Causality Graph

Notes

- Causality graph has 11 events - problems and symptoms
- Mark all nodes that have only emerging directed edges as problems - Nodes 1, 2, and 11
- Other nodes are symptoms

P-S Causality Graph

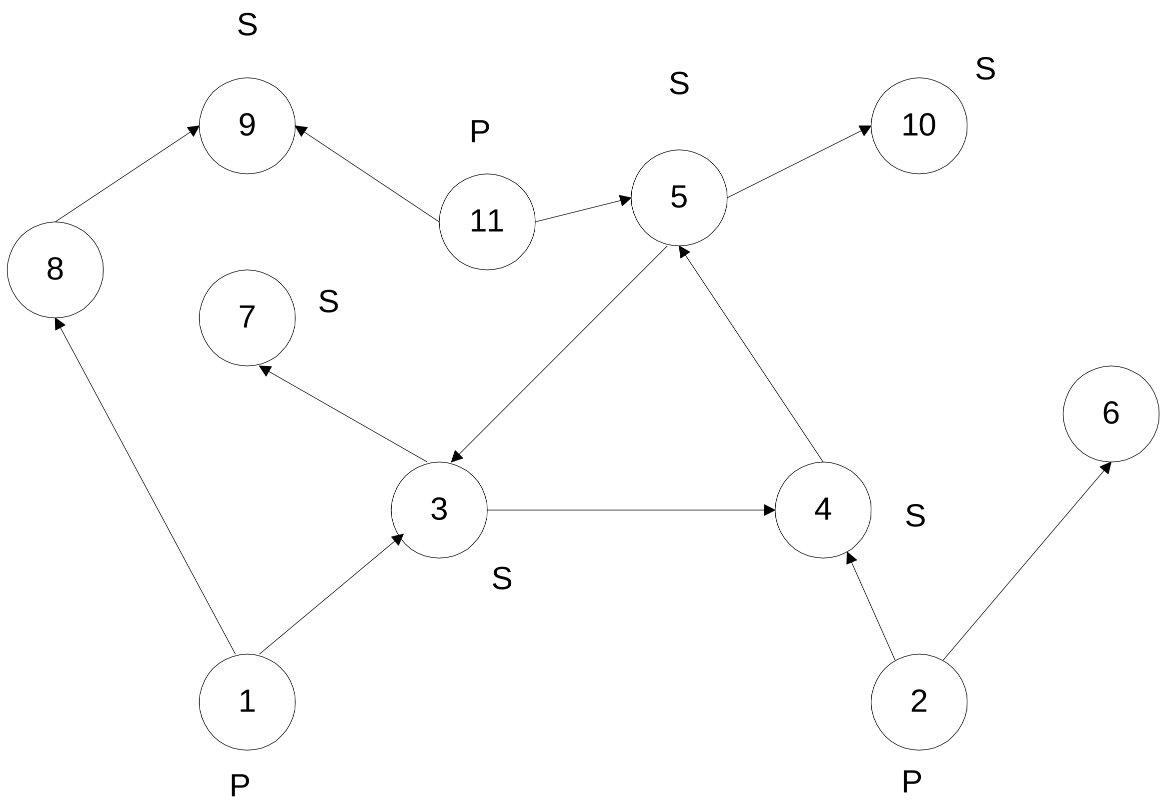


Figure 11.24(b) Problem-Symptom Causality Graph

Figure 11.24 Generalized Causality Graph

Notes

- To reduce causality graph to correlation graph:
  - Symptoms 3, 4, and 5 are cyclical: replace with one symptom, say 3
  - S7 and S10 are caused by S3 and S5 and hence ignored
  - S8 causes S9. Keep S9 and eliminate S8; reason for this would be more obvious if we go through reduction of codebook to correlation matrix

Correlation Graph and Matrix

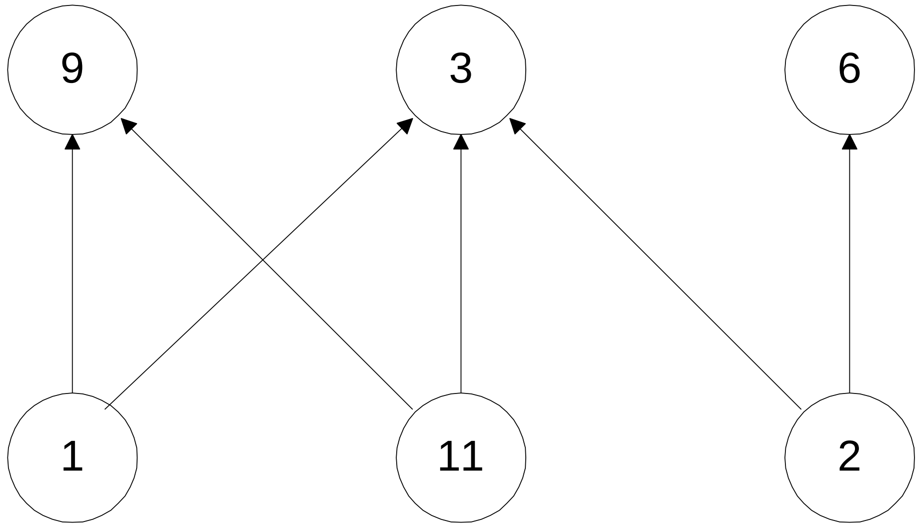


Figure 11.25 Correlation Graph for Figure 11.24

Notes

	P1	P2	P11
S3	1	1	1
S6	0	1	0
S9	1	0	1

Figure 11.26 Correlation Matrix for Figure 11.24

- Note that problems 1 and 11 produce identical symptoms

Codebook Enhancements

- Codebook described so far assumes Hamming distance of 1 for uniqueness
- Noise affects accuracy
- Increase Hamming distance to >1
- Probability of a problem causing a symptom assumed as 1. It can be made Si = Pr(Pj) to be more realistic

Notes

State Transition Model

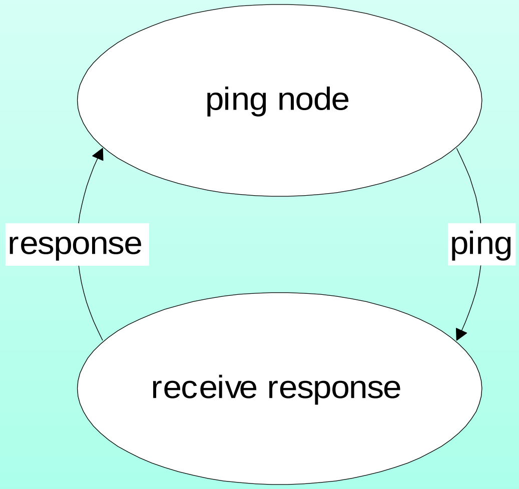
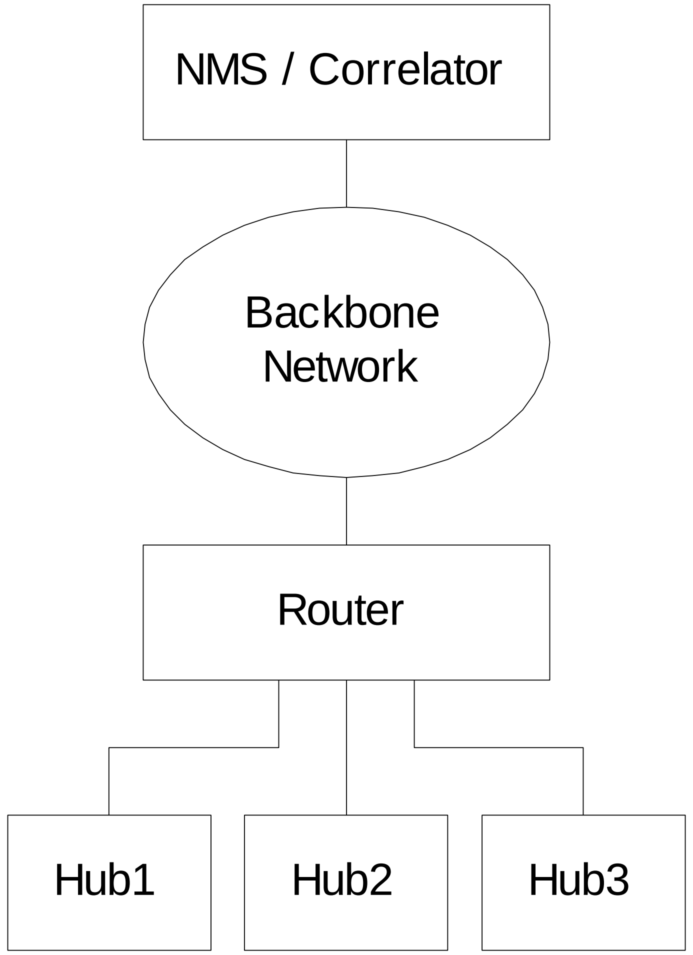


Figure 11.27 State Transition Diagram for Ping/Response

Notes

- Used in Seagate’s NerveCenter correlation system
- Integrated in NMS, such as OpenView
- Used to determine the status of a node

State Transition Model Example



Physical Network

Notes

- NMS pings hubs every minute
- Failure indicated by the absence of a response

State Transition Graph

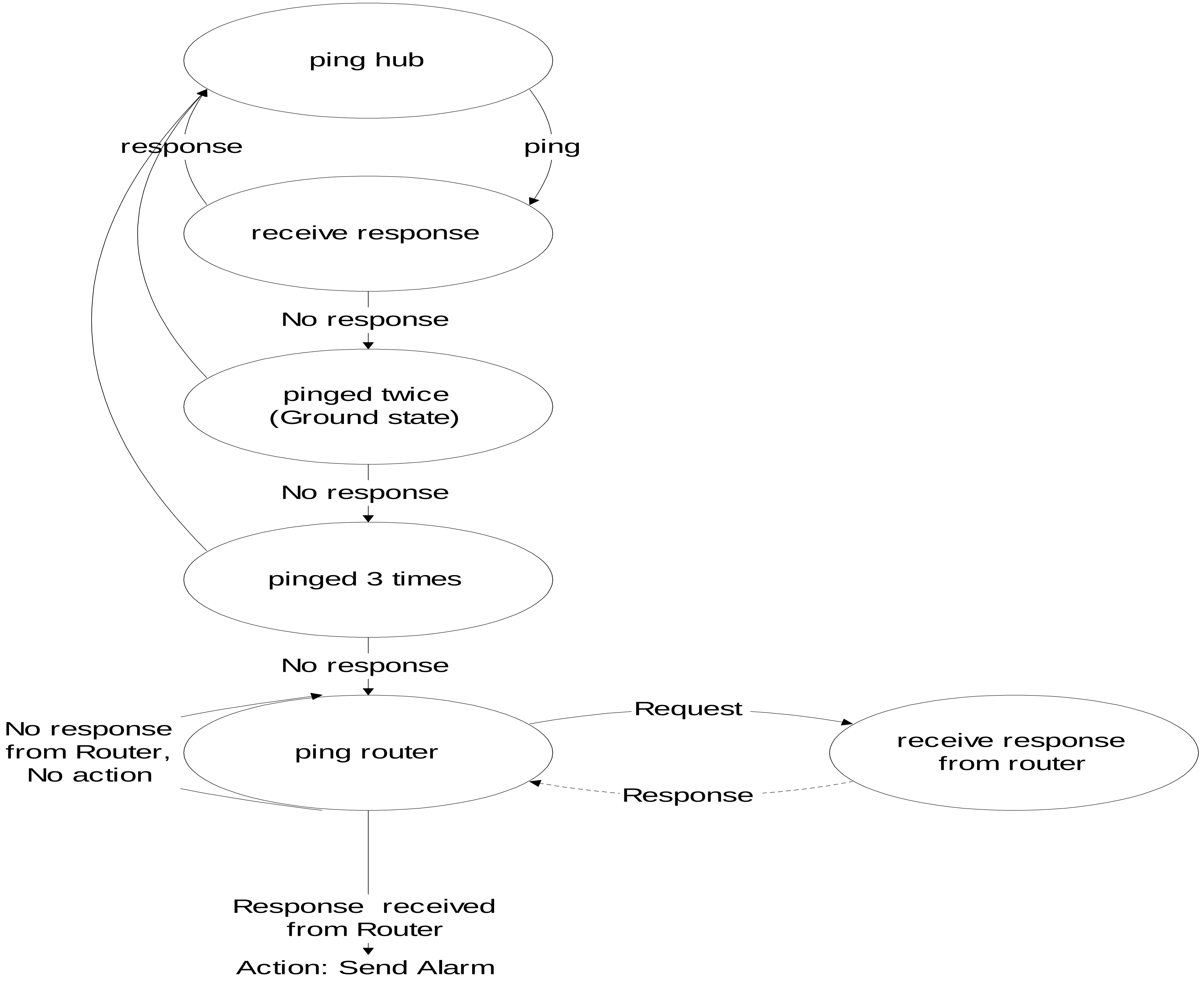


Figure 11.28 State Transition Graph Example

Finite State Machine Model

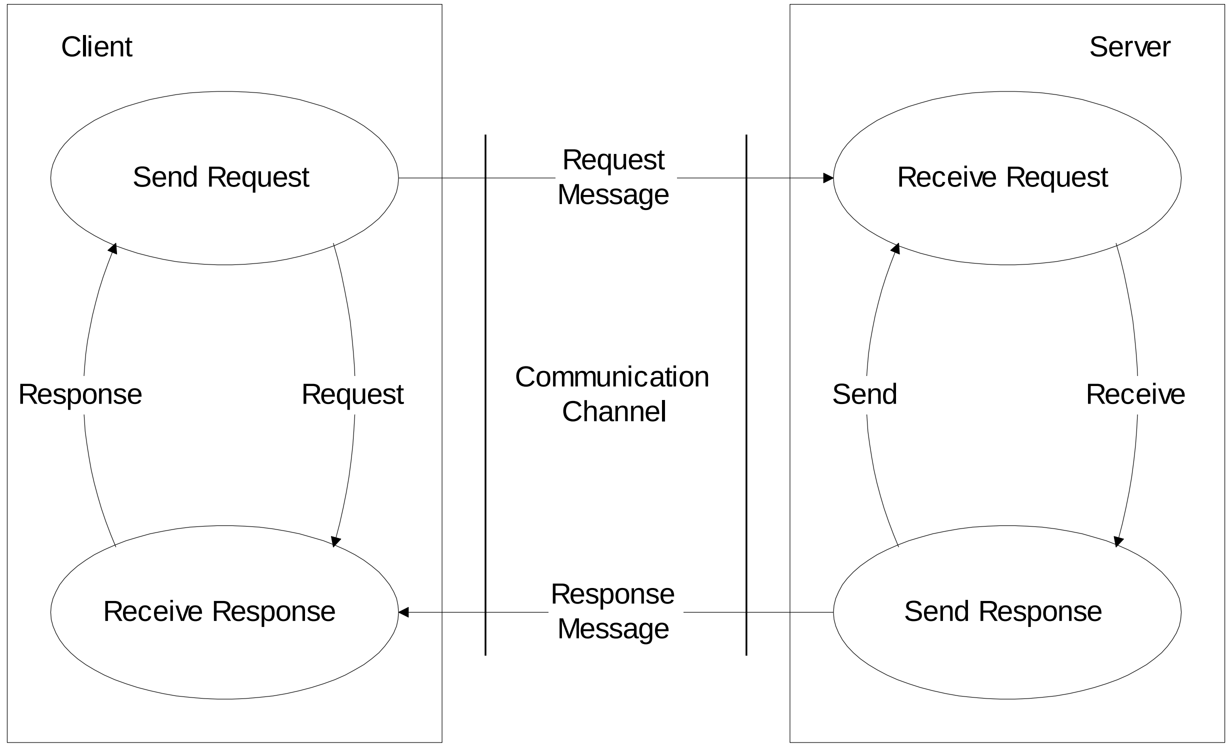


Figure 11.29 Communicating Finite State Machine

Notes

- Finite state machine model is a passive system; state transition graph model is an active system
- An observer agent is present in each node and reports abnormalities, such as a Web agent
- A central system correlates events reported by the agents
- Failure is detected by a node entering an illegal state

Security Management

- Security threats
- Policies and Procedures
- Resources to prevent security breaches
- Firewalls
- Cryptography
- Authentication and Authorization (Differences ???)
- Client/Server authentication system
- Message transfer security
- Network protection security

Notes

Security Threats

Masquerade= pretend to be someone one is not.

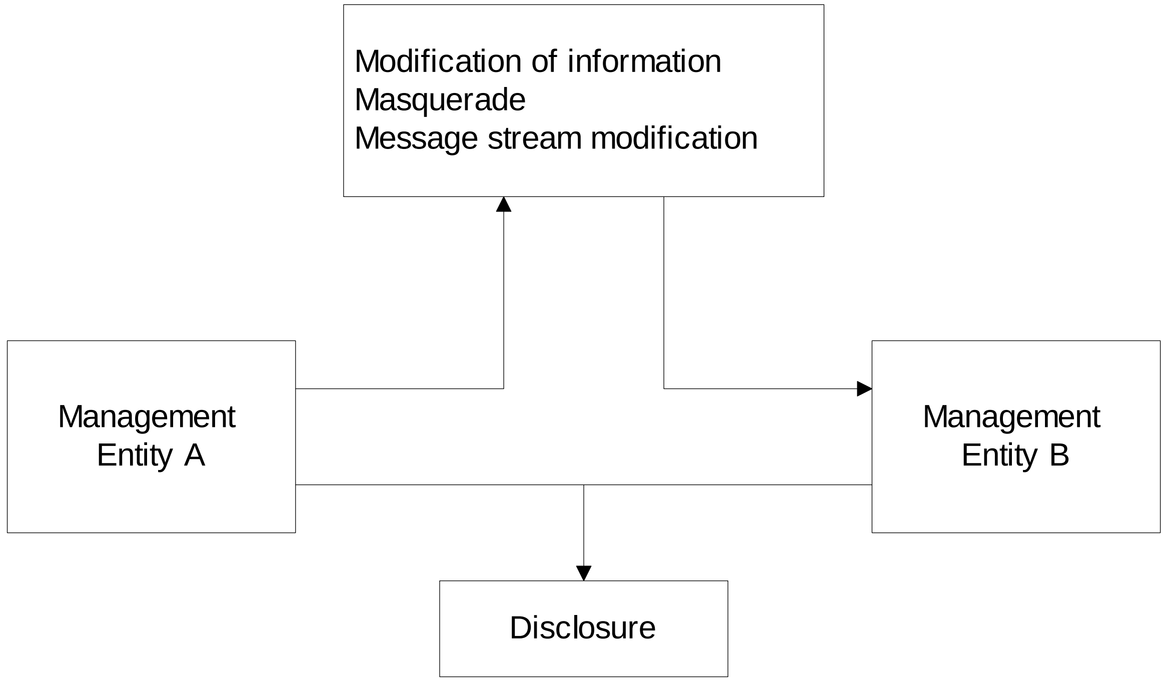


Figure 7.10 Security Threats to Management Information

Notes

- SNMPv3 addressed security threats using USM (user-based security model)
- USM has two modules:
  - Authentication module
    - Data integrity
    - Data origin
  - Privacy module
    - Data confidentiality
    - Message timeliness
    - Message protection

[Security] Policies and Procedures

Basic guidelines to set up policies and procedures:

1. Identify what you are trying to protect.
2. Determine what you are trying to protect it from.
3. Determine how likely the threats are.
4. Implement measures, which will protect your assets in a cost-effective manner.
5. Review the process continuously and make improvements to each item if a weakness is found.

Notes

- References:
  - Formal statement of rules for protecting organization’s technology and assets (RFC 2196)
  - Introduction to Firewalls (NIST)
  - Orange Book by National Computer Security Center (NCSC) rates computers based on security design features

Secure Communication Network

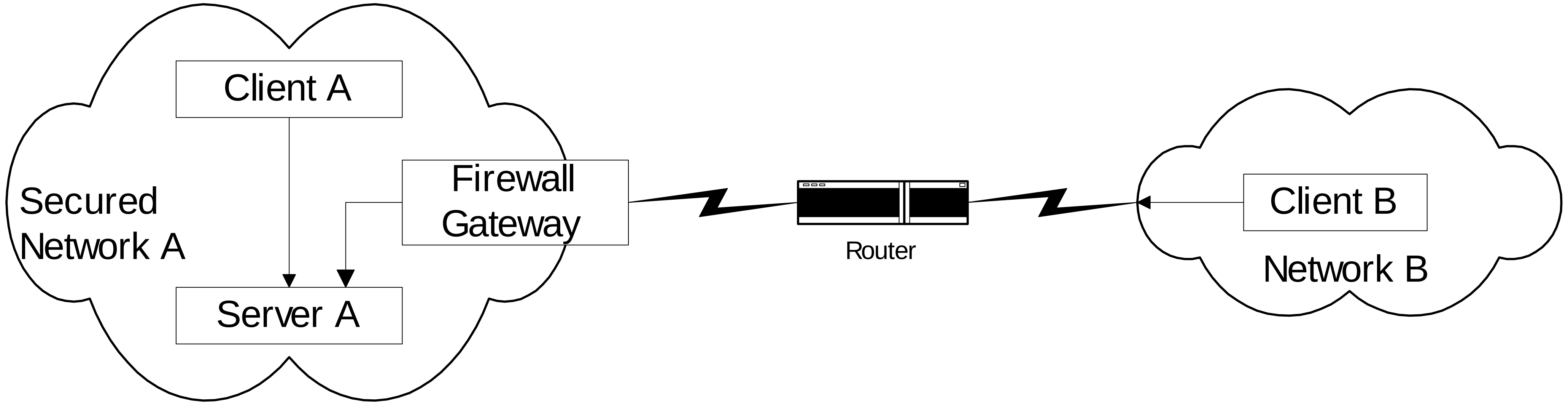


Figure 11.30 Secure Communication Network

Notes

- Firewall secures traffic in and out of Network A
- Security breach could occur by intercepting the message going from B to A, even if B has permission to access Network A
- Most systems implement authentication with user id and password
- Authorization is by establishment of accounts

Firewalls

- Protects a network from external attacks
- Controls traffic in and out of a secured network
- Could be implemented in a router, gateway, or a special host
- Benefits
  - Reduces risks of access to hosts
  - Controlled access
  - Eliminates annoyance to the users
  - Protects privacy (e.g., finger)
  - Hierarchical implementation of policy and and technology (e.g., finger)

Notes

Packet Filtering Firewall

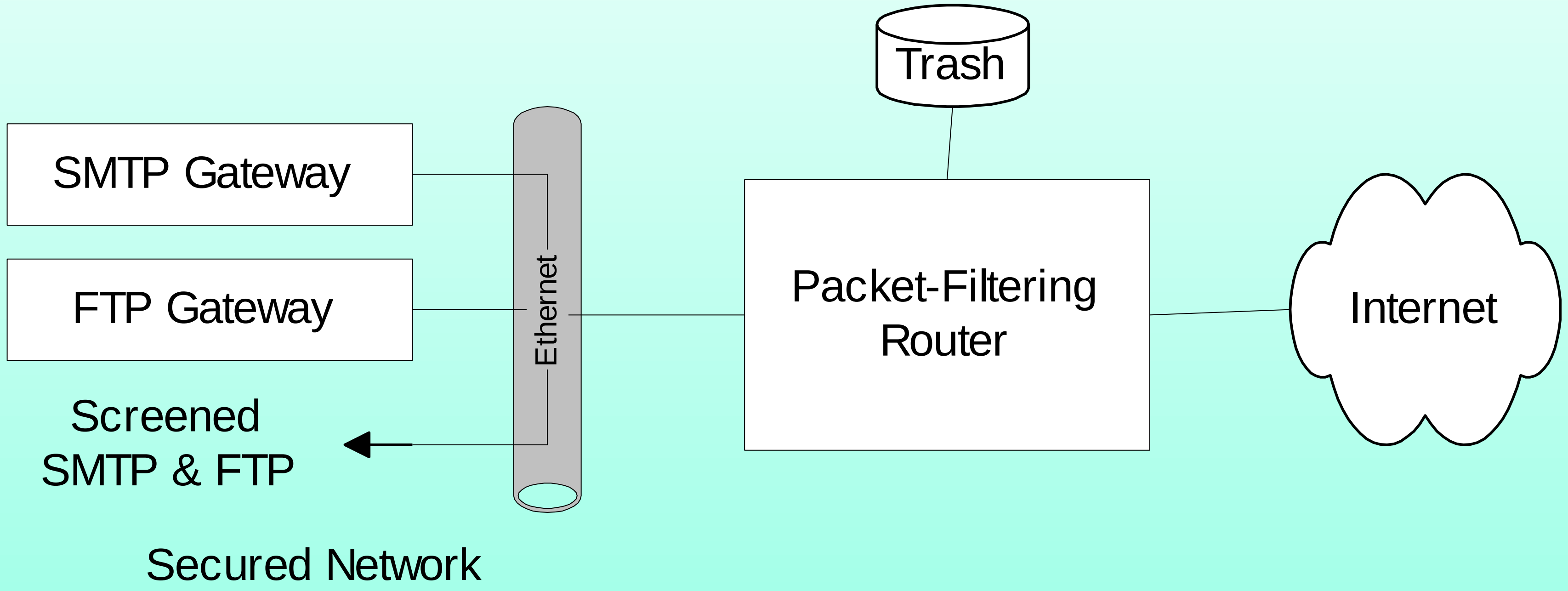


Figure 11.31 Packet-Filtering Router

Notes

- Uses protocol specific criteria at **DLC**, network, and transport layers
- Implemented in routers - called screening router or packet-filtering routers
- Filtering parameters:
  - Source and/or destination IP address
  - Source and/or destination TCP/UDP port address, such as ftp port 21
- Multistage screening - address and protocol
- Works best when rules are simple

In the OSI networking model, Data Link Control (DLC) is the service provided by the data link layer.

Application Level Gateway

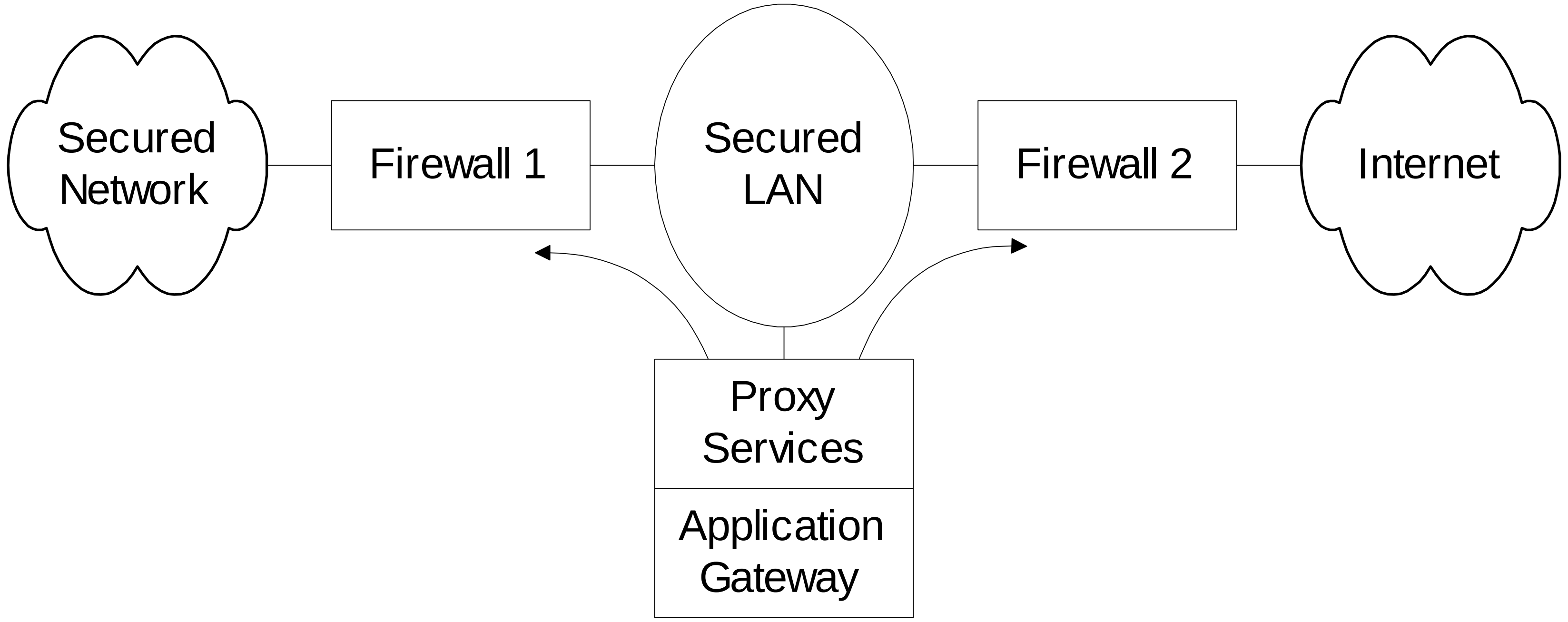


Figure 11.32 Application Level Gateway

Notes

- Firewalls 1 and 2 route traffic only from and to the secured LAN
- Secured LAN is gateway LAN
- Behavior of application gateway dependent on the application
- FTP traffic stored and forwarded after validation
- TELNET hosts validated for the session and then direct communication established

Cryptography

- "Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. It includes encrypting a message by its sender and decrypting it by its destination"

- Secure communication requires
  - Integrity protection: ensuring that the message is not tampered with
  - Authentication validation: ensures the originator identification

- Security threats
  - Modification of information
  - Masquerade
  - Message stream modification
  - Disclosure

- Hardware and software solutions for security threats

- Most secure communication is software based

Secret Key Cryptography

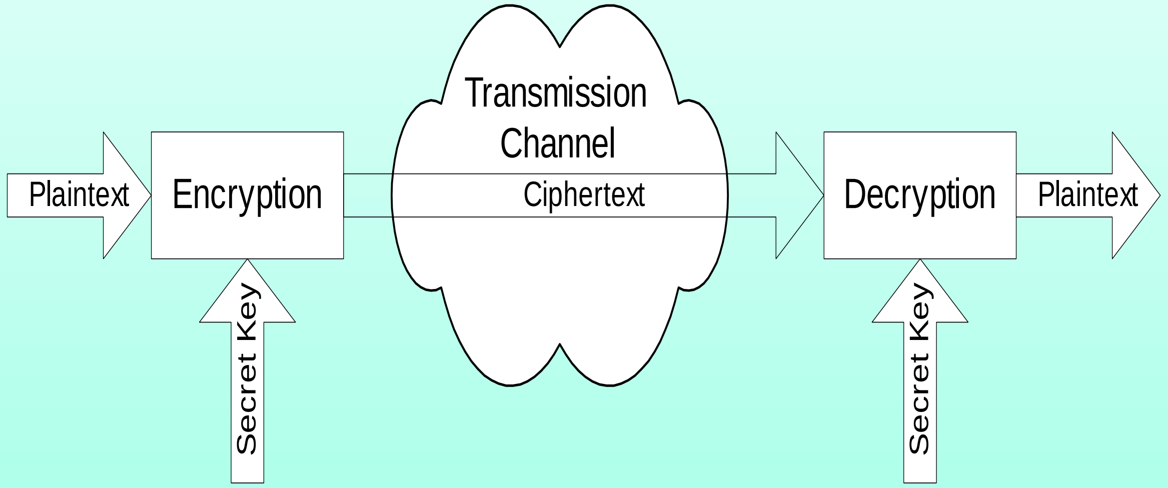


Figure 11.33 Basic Cryptographic Communication

A cipher= a secret or disguised way of writing; a code; the resulting message of the encryption

Notes

- Caesar cipher: each letter replaced by another letter, which is three letters behind in the alphabet
  - – Maximum of 26 attempts to decode Caesar cipher
- Monoalphabetic cipher: Replace a letter with another randomly chosen; Maximum attempts to decode 26!
- One secret key is needed between each pair

- Two standard algorithms for secret key:
  - DES (Data Encryption Standard): 64-bit message blocks and 56-bit key
  - IDEA (International Data Encryption Algorithm): 64-bit message blocks and 128-bit key
- Message block derived using CBC (Cipher Block Chaining)
  - – Principle based on rearranging the blocks several times based on predetermined algorithm and secret key

Public Key Cryptography

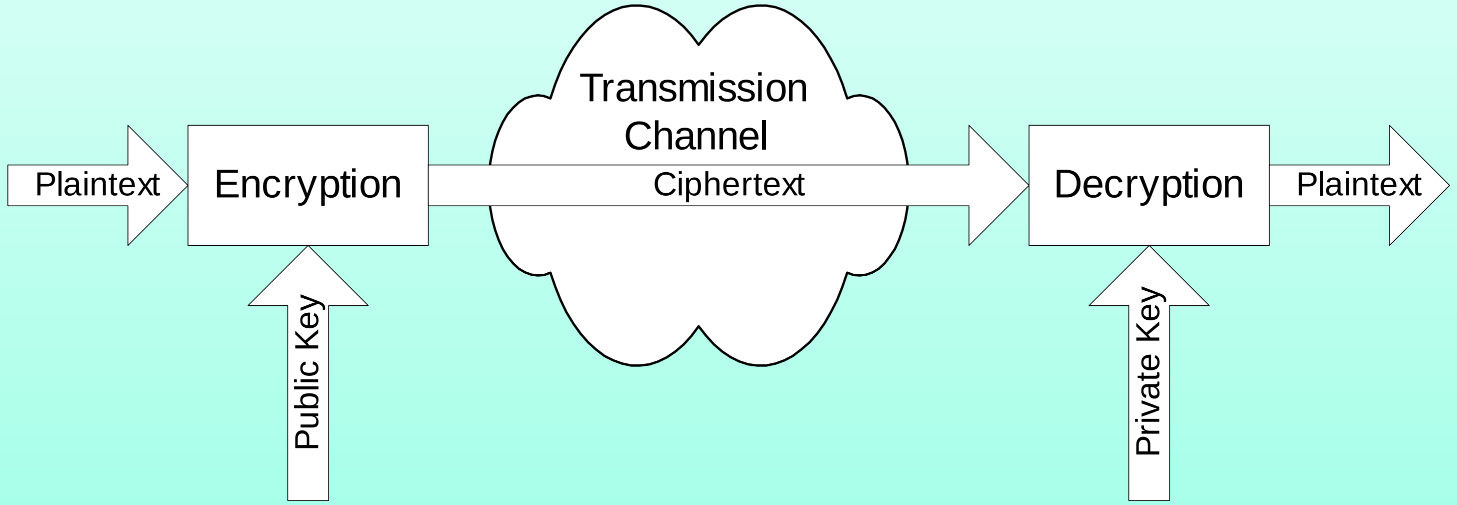


Figure 11.34 Public Key Cryptographic Communication

Notes

- Asymmetric cryptography - public and private key
- Public key is distributed by the receiver to the senders to encrypt the message.
- Private key is used by receiver to decode ciphertext
- Mailbox analogy
- Commonly used public key is RSA (Rivest, Shamir, and Adleman); 512-bit key, variable block size
- RSA less efficient than DES and IDEA; used to encrypt secret key

Message Digest

- **Message digest is a cryptographic hash algorithm added to a message**

- One-way function
- Analogy with CRC
- If the message is tampered with, the message digest at the receiving end fails to validate
- MD5 (used in SNMPv3) commonly used MD
- MD5 takes a message of arbitrary length (32-byte) blocks and generates 128-bit message digest
- SHS (Secure Hash Standard) message digest proposed by NIST handles 2^{64} bits and generates 160-bit output

Notes

Example:

```
$ md5
The quick brown fox jumped over the lazy dog
^D
d8e8fca2dc0f896fd7cb4cb0031ba249
```

Digital Signature

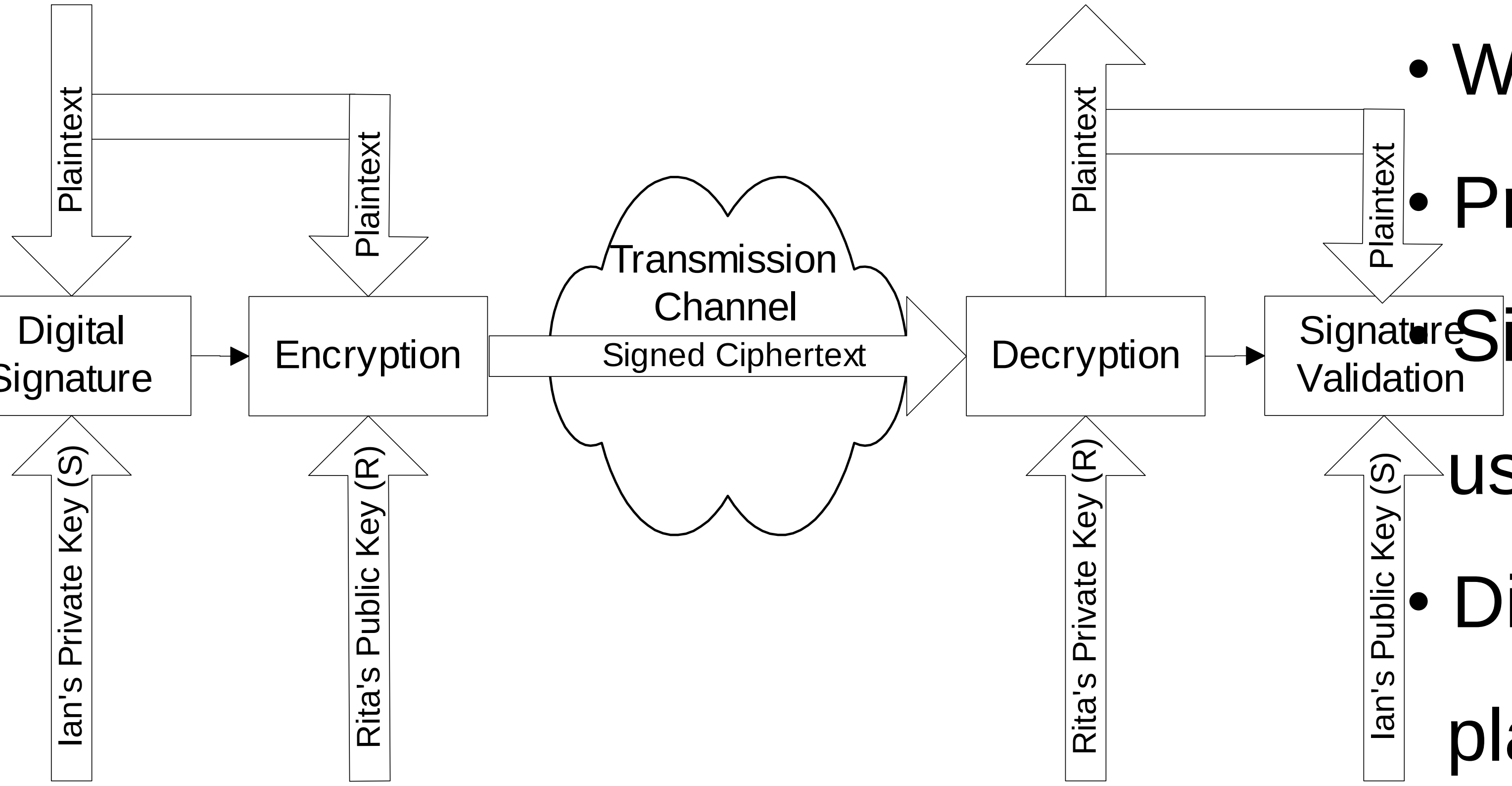


Figure 11.37 Signed Public-Key Cryptographic Communication

Notes

- Why do we need digital signature?
- Principle reverse of public key
- Signature created using private key and validated using public key
- Digital signature is a message digest generated from plaintext and private key by a hashing algorithm
- Digital signature is concatenated with the plaintext and encrypted using public key

Authentication and Authorization

- Authentication verifies user identification
    - Client/server environment
        - Ticket-granting system
        - Authentication server system
        - Cryptographic authentication
    - Messaging environment
        - e-mail
        - e-commerce
- Authorization grants access to information
    - Read, read-write, no-access
    - Indefinite period, finite period, one-time use

Ticket-Granting System

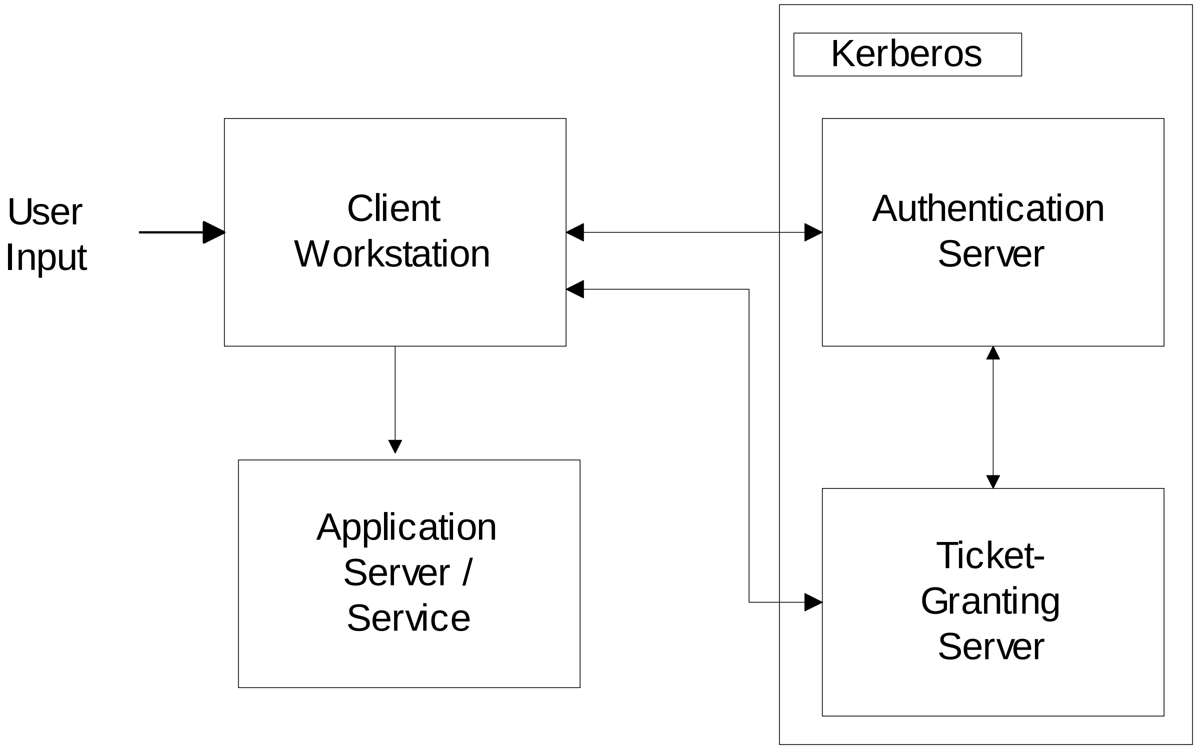


Figure 11.38 Ticket-Granting System

Notes

- Used in client/server authentication system
- Kerberos developed by MIT
- Steps:
  - User logs on to client workstation
  - Login request sent to authentication server
  - AS checks ACL, grants encrypted ticket to client
  - Client obtains from TGS service-granting ticket and session key
  - Application Server validates ticket and session key, and then provides service

Authentication Server

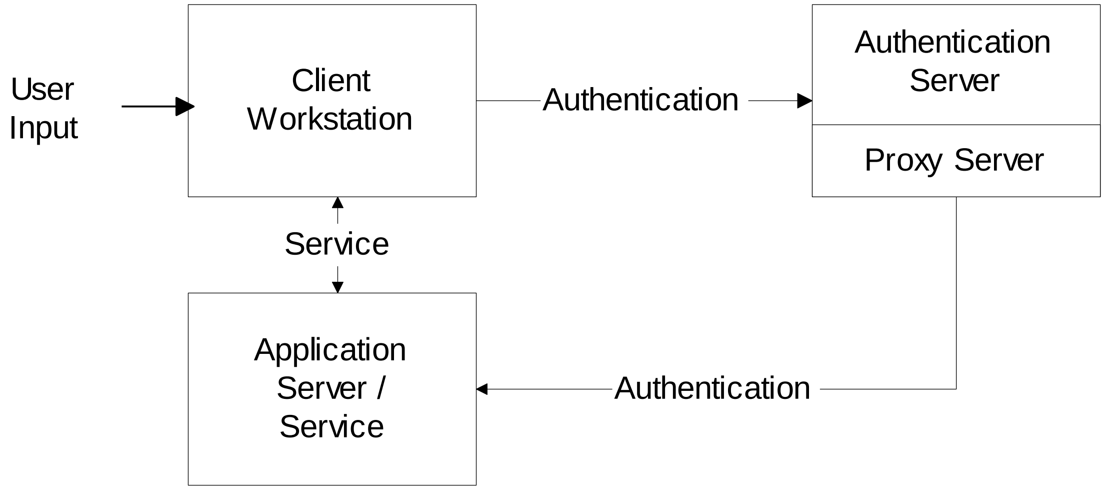


Figure 11.39 Authentication Server

Notes

- Architecture of Novell LAN
- Authentication server does not issue ticket
- Login and password not sent from client workstation
- User sends id to central authentication server
- Authentication server acts as proxy agent to the client and authenticates the user with the application server
- Process transparent to the user

Message Transfer Security

- Messaging one-way communication
- Secure message needs to be authenticated and secured
- Three secure mail systems
  - Privacy Enhanced Mail (PEM)
  - Pretty Good Privacy (PGP)
  - X-400: OSI specifications that define framework; not implementation specific

Notes

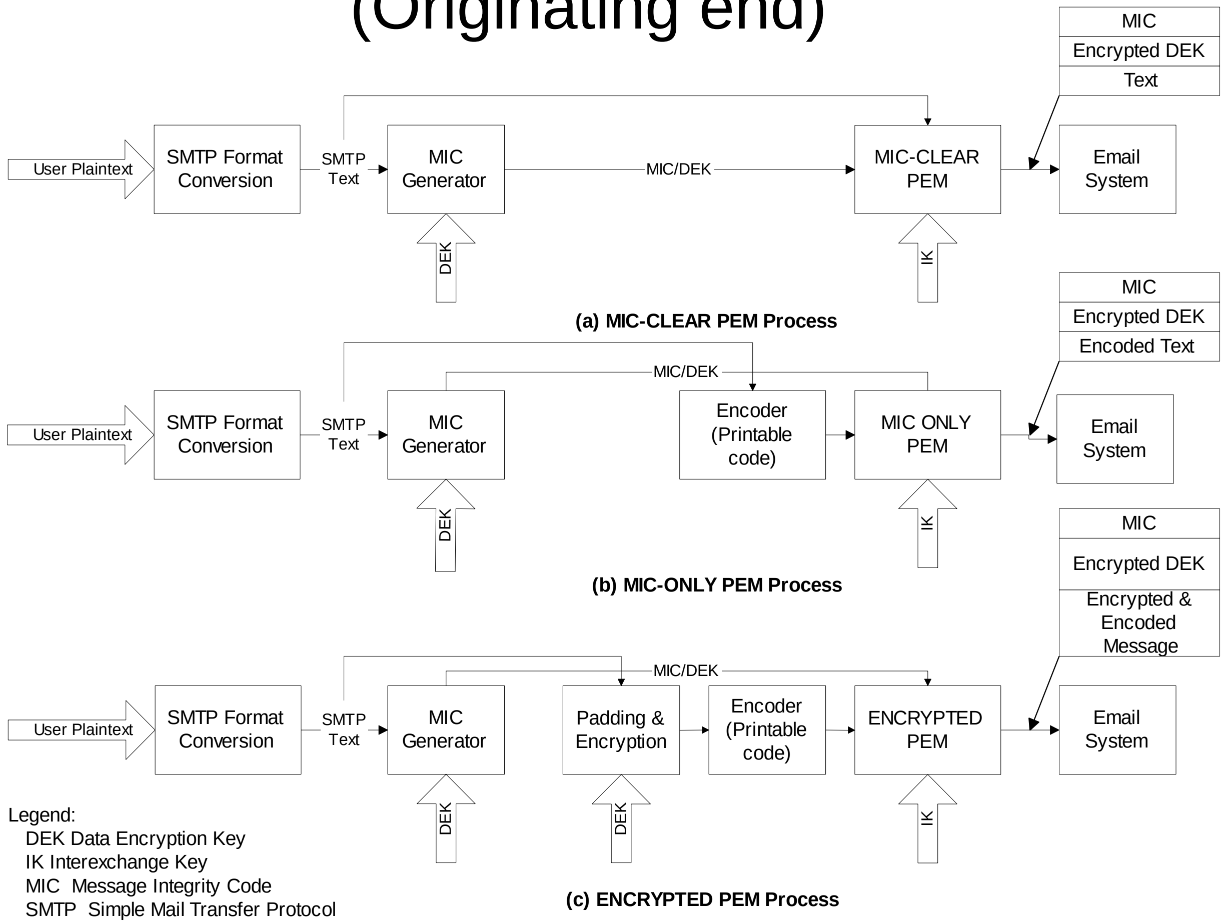
Privacy Enhanced Mail

- Developed by IETF (RFC 1421 - 1424)
- End-to-end cryptography
- Provides
  - Confidentiality
  - Authentication
  - Message integrity assurance
  - Nonrepudiation of origin
- Data encryption key (DEK) could be secret or public key-based originator and receiver agreed upon method
- PEM processes based on cryptography and message encoding
  - MIC-CLEAR (Message Integrity Code-CLEAR)
  - MIC-ONLY
  - ENCRYPTED

Notes

PEM Processes

(Originating end)



(a) MIC-CLEAR PEM Process

(b) MIC-ONLY PEM Process

(c) ENCRYPTED PEM Process

Figure 11.40 PEM Processes

Notes

- DEK a random number generated per message basis: used to encrypt the message text and generate MIC
- IK a long-range key agreed upon between the sender receiver used to encrypt DEK: IK is either public or secret
- Public key avoids repudiation

Pretty Good Privacy

(Originating end)

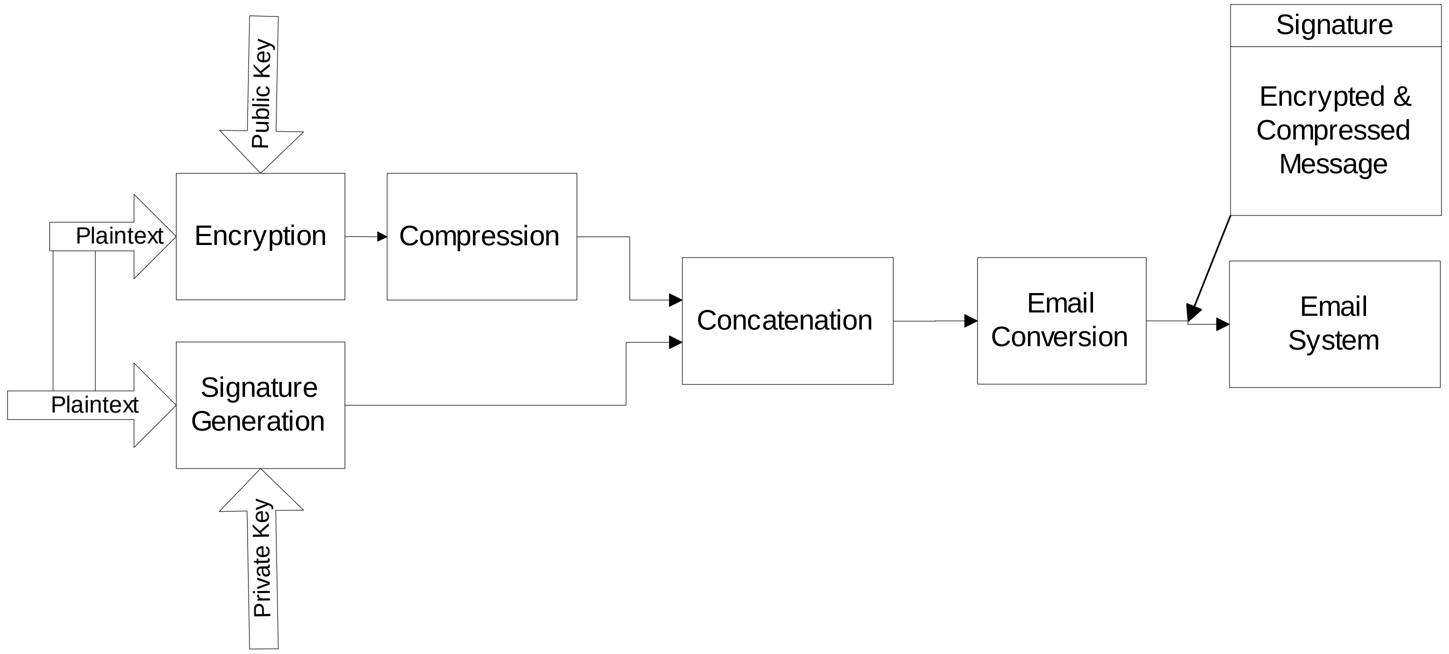


Figure 11.41 PGP Process

Notes

- PGP secure mail package developed by Zimmerman
- Available in public domain
- Signature generation
  - Uses MD5 to generate hash code
  - Encrypts hash code with sender’s private key using RSA algorithm
- Encryption of the message done using IDEA or RSA
- Compression done with ZIP
- email conversion done using Radix-64
- PGP similar to encrypted PEM with added compression

SNMPv3 Security

(Outgoing message)

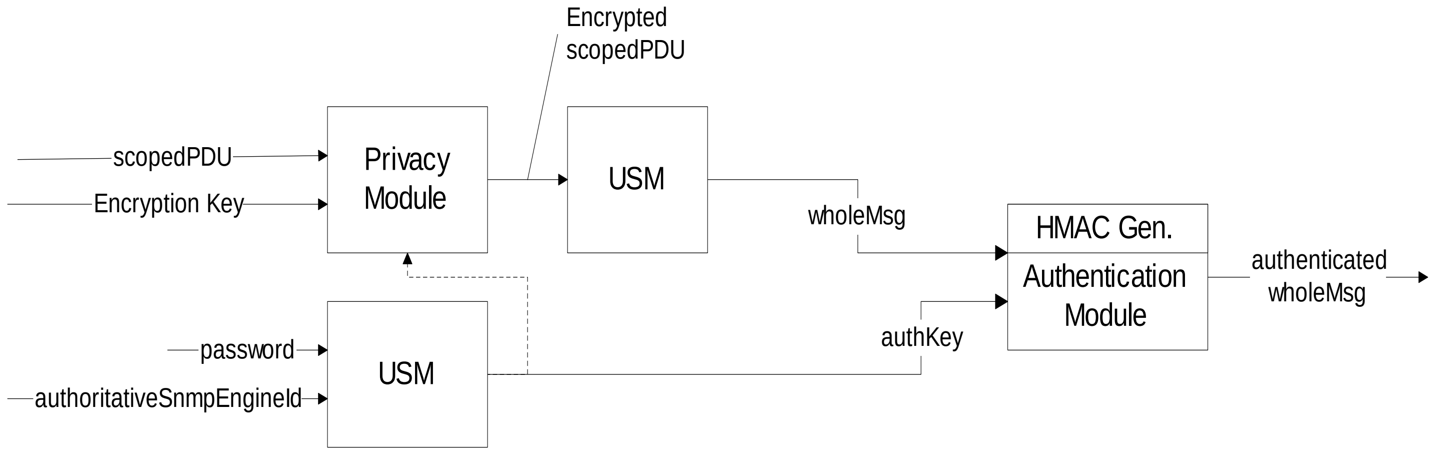


Figure 11.42 SNMP Secure Communication

In cryptography, a **keyed-hash message authentication code**(**HMAC**) is a specific type ofmessage authentication code(MAC) involving a cryptographic hash function (hence the 'H') in combination with a secretcryptographic key.

Notes

- Authentication key equivalent to DEK in PEM or private key in PGP
- Authentication key generated using user password and SNMP engine id
- Authentication key may be used to encrypt message
- USM prepares the whole message including scoped PDU
- HMAC, equivalent of signature in PEM and PGP, generated using authentication key and the whole message
- Authentication module provided with authentication key and HMAC to process incoming message

Virus Attacks

- Executable programs that make copies and insert them into other programs
- Attack hosts and routers
- Attack infects boot track, compromises cpu, floods network traffic, etc.
- Prevention is by identifying the pattern of the virus and implementing protection in virus checkers

Accounting Management

- Least developed application
- Usage of resources
- Hidden cost of IT usage (libraries)
- Functional accounting
- Business application

Notes

Report Management

Table 11.1 Planning and Management Reports

Category	Reports
Quality of service / Service level agreement	Network availability Systems availability Problem reports Service response Customer satisfaction
Traffic trends	Traffic patterns Analysis of internal traffic volume Analysis of external traffic volume
Technology trends	Current status Technology migration projection
Cost of Operations	Functional Usage Personnel

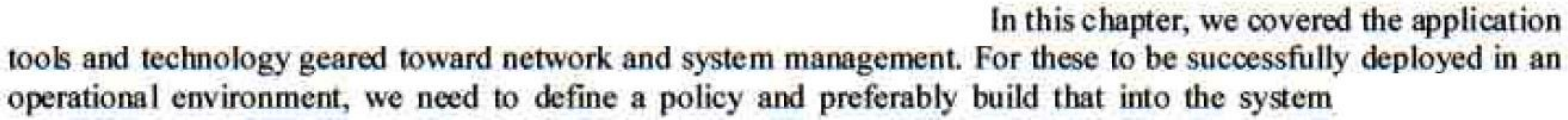
Table 11.2 System Reports

Category	Reports
Traffic	Traffic load - internal Traffic load - external
Failures	Network failures System failures
Performance	Network Servers Applications

Table 11.3 User Reports

Category	Reports
Service level agreement	Network availability System availability Traffic load Performance
User specific reports	User-defined reports

Policy-Based Management



In this chapter, we covered the application tools and technology geared toward network and system management. For these to be successfully deployed in an operational environment, we need to define a policy and preferably build that into the system

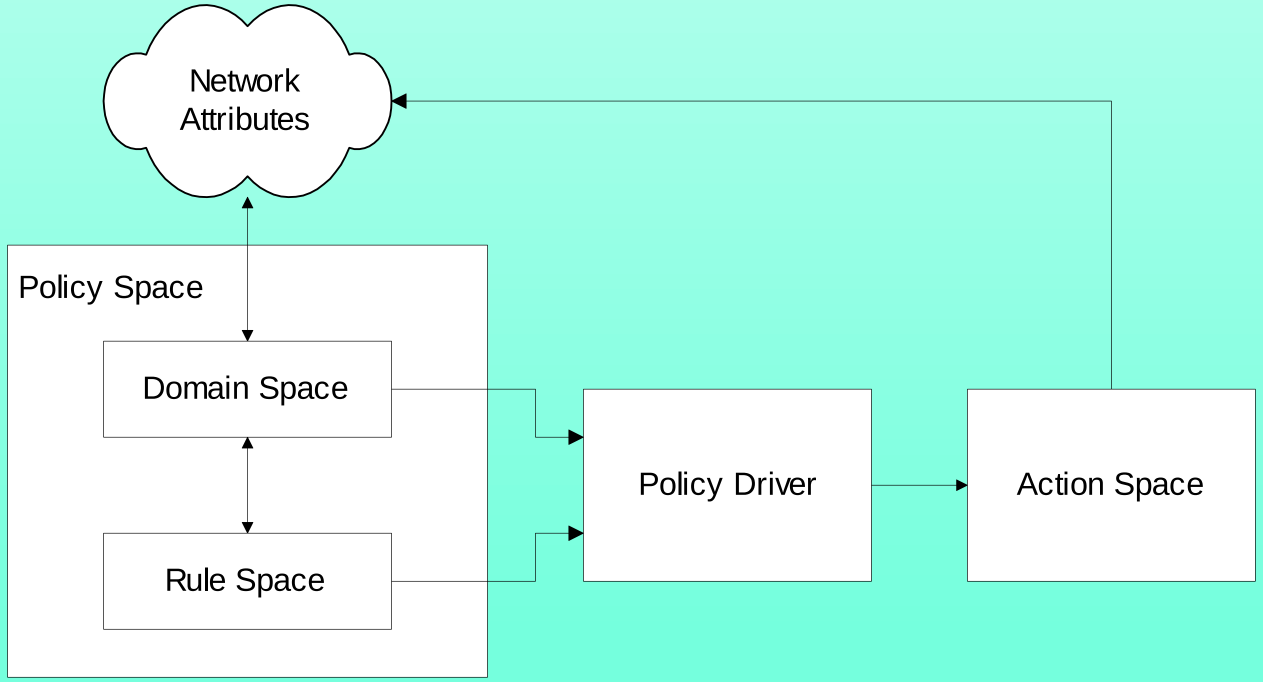


Figure 11.43 Policy Management Architecture

Notes

- Domain space consists of objects (alarms with attributes)
- Rule space consists of rules (if-then)
- Policy Driver controls action to be taken
- Distinction between policy and rule; policy assigns responsibility and accountability
- Action Space implements actions

Service Level Management

- SLA (**Service level agreement**) management of service equivalent to QoS of network

- SLA defines
  - Identification of services and characteristics
  - Negotiation of SLA
  - Deployment of agents to monitor and control
  - Generation of reports

- SLA characteristics
  - Service parameters
  - Service levels
  - Component parameters
  - Component-to-service mappings

Notes